Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100

COMMENTS OF MOTOROLA SOLUTIONS, INC.

Chuck Powers
Director,
Engineering and Technology Policy
Motorola Solutions, Inc.
1455 Pennsylvania Avenue, N.W.
Washington, DC 20004
(202) 371-6900

April 11, 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Motorola Solutions, Inc. ("MSI") whole-heartedly supports the vision of a nationwide network of interoperable regional and tribal communications systems operating in the public safety broadband spectrum. The Commission has an important role to play in ensuring the nationwide interoperability of the public safety network. The selection of 3GPP's Long Term Evolution ("LTE") standard as the technological platform for the public safety broadband network, which is overwhelmingly supported by the public safety community, will be crucial to serving this goal. Motorola Solutions also believes, however, that state, local, and tribal public safety officials must have an active role in designing, implementing, and management of the new network, as they will have the most relevant experience with public safety communications on the local level.

The Commission should continue to promote interoperability and the development of advanced functionality within the network by setting only the high level framework requirements of the nationwide network and allowing the public safety community sufficient flexibility and autonomy to design and construct the network to meet their needs. While the *Fourth Further Notice* asks many relevant questions about the design and operations of the public safety broadband network, MSI believes that the Commission would do well to refrain from codifying the specific technical and operational details of the network into its rules. Relegating these technical characteristics to the regulatory process will ultimately hinder the ability of public safety network operators to quickly adopt and implement the most advanced interoperable technologies available to them.

To achieve this vision, Motorola Solutions makes the following recommendations:

- The Commission should develop a uniform nationwide architectural framework for the public safety broadband network that identifies the guiding principles of the network's development and the basic requirements for interoperability while preserving the maximum flexibility for public safety in implementation.

- As the Commission examines a national governance structure for the network, it should be attentive to concerns about the speed and cost of broadband deployment, and emphasize regional, tribal, and local control over the planning and oversight of broadband deployment, within the requirements for interoperability.

- While it is unnecessary for the Commission to mandate specific roaming configurations or to set forth model agreements, it is essential that 700 MHz public safety broadband users be able to roam across all 700 MHz public safety broadband network deployments.

- Federal use of the network should be encouraged and authorized Federal users should be able to roam throughout the nationwide network.

- Regional, tribal, and local public safety authorities should have the ability to decide which entities, including secondary responders, should be given access to the network in order to protect the safety of life, health, or property.

- To best achieve the goal of a nationwide public safety broadband network while ensuring public safety has access to mission critical narrowband communications, all costs for relocation of narrowband 700 MHz public safety operations should be reimbursed.

To supplement these comments, and to provide the Commission with the most detailed information possible to guide its decision making, Motorola Solutions has also included a Technical Appendix that discusses many of the specific questions asked in the *Fourth Further Notice*.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100

COMMENTS OF MOTOROLA SOLUTIONS, INC.

Motorola Solutions, Inc. ("MSI") hereby responds to the Fourth Notice of Proposed Rule Making in the above-captioned proceeding designed to create an effective technical framework for ensuring the deployment and operation of a nationwide interoperable public safety broadband network.[1]

I. INTRODUCTION.

For more than 75 years, MSI has pursued a core mission to provide public safety agencies with advanced communications tools that help save lives and property. MSI's experience in working collaboratively with public safety officials has provided MSI with valuable insight into the benefits of deploying interoperable networks for public safety users, and the need for effective governance models for multi-agency systems that enables both interoperability and effective local operations.

[1] *See* Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, *et al.*, WT Docket No. 06-150, PS Docket No. 06-229, WP Docket No. 07-100, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 26 FCC Rcd 733 (2011) ("*Fourth Notice*").

MSI supports the vision of an interoperable nationwide network comprised of interoperable, regional or tribal systems operating in the public safety broadband spectrum.[2] While various models for governance of the nationwide Public Safety Broadband Network ("PSBN") with varying levels of national control and coordination are conceivable, MSI believes that consideration must be given to how quickly such a structure or entity could be established and functional, so as not to delay broadband deployment. Whatever governing body is ultimately chosen, MSI believes it critical that it is responsive and representative of the ultimate end users of the network and their operational requirements. State and local officials are better positioned than national officials to determine what applications or quality of services is best for them, because of their greater operational experience in managing sophisticated communications networks.

MSI applauds the work of the FCC in this proceeding and agrees that interoperability is essential to the success of providing nationwide public safety broadband services. Enabling service to roaming public safety officers is key for all networks. Each regional public safety broadband network also will have requirements that will demand at least some level of customization on top of the list of standardized features and applications set for nationwide interoperability. This aspect of the network is important to meet local and regional needs. It will also help drive competition among vendors to provide innovative solutions for the betterment of public safety communications. With the right regulatory framework, it is possible to achieve both nationwide interoperability and local control. These are not mutually exclusive

[2] In the context of these comments "regional" could encompass a group of localities, a state or multiple states.

objectives but, rather, can be complementary given the foundation of advanced broadband technology.

MSI recommends that the Commission set only those requirements necessary to ensure interoperability across the public safety broadband regional deployments. This approach will allow the PSBN to develop according to the needs of the users, while also providing an interoperable foundation upon which the nationwide interoperable public safety network can be built.

Reliance on 3GPP's Long Term Evolution ("LTE") standard as the technological platform for the PSBN is overwhelmingly endorsed and supported by the public safety community and industry. It is important to consider, however, that LTE is a relatively new standard for both public safety and commercial operators that will be subject to substantial revisions and enhancements in the future through the industry standards setting process. Because it is principally a commercial-based standard, LTE should offer public safety with faster technology refresh cycles, a benefit that users have identified as important. However, this benefit will be undermined if manufacturers and operators must first wait for regulatory "notice and comment" rule making proceedings to be completed each time an LTE network component or feature is added to the existing standard or to existing products. More flexible, independent oversight and regulation of the interoperable components of the network is needed.

In these comments, MSI offers its perspective on some of the most significant aspects of the Fourth Notice. Additional comments on the technical aspects of the Fourth Notice related to defining interoperability at the physical layer, network layer and application layer are included in the attached technical appendix.

II. THE COMMISSION SHOULD DEVELOP A UNIFORM NATIONWIDE ARCHITECTURAL FRAMEWORK.

The Commission should develop a uniform nationwide architectural framework that ensures that basic requirements for interoperability are met while also enabling regional, tribal, and local control over public safety broadband network design and deployment. To meet the needs of public safety, any interoperability framework must allow for regional, tribal, or local operational management. Public safety's operating procedures revolve around local/regional Computer Aided Dispatch (CAD) and incident command structures. New broadband applications and services need to be integrated into those local/regional workflow procedures. Just as voice systems are mission critical today, MSI expects that in the future, added capabilities for data access and imaging/video will also become mission critical tools to support prevention and response.

It is important to consider the various functions and elements required for interoperability together with the entities and processes best-suited to fulfilling these required functions, consistent with the need to preserve regional, tribal, and local operational control. National uniformity on certain aspects will be essential for interoperability. At the same time, most use of the network on a day-to-day basis will be local and those functions most pertinent to the local control of bearer traffic should be located at the locality, region, tribal area, or state deploying the network in that area. Doing so enhances sustainability of the network and reduces costs.

LTE cores are a small fraction of overall deployment costs and will be reduced even further as low cost small scale cores emerge. The initial costs of locating cores closer to the local traffic are recouped by reduced backhaul costs. This helps avoid the "tromboning" approach of routing traffic from regional cell sites to a far distant core and

back to the local agencies over a national backbone. Regionally based cores also allow a first responder to access both local and national applications from anywhere within the nationwide network as needed and as authorized. Interoperability with the 911 PSAP, current land mobile systems and Next Generation 911 would also be enhanced as the network and functions are locally/regionally based.

Identifying a consistent national architectural framework will promote clarity and stability in public safety broadband deployment. Currently, the rules and requirements for public safety broadband waiver recipients are set forth in at least three different decisions from the Commission and the Bureau. While these decisions are generally consistent with each other, they are not identical and this creates a situation where the risk for confusion or incompatibility is increased. System rules and architectural requirements should be stabilized with enough lead time to allow manufacturers and users to finalize their requirements for specific equipment designs and deployment. Any perceived lack of stability or inconsistency in the system requirements could lead to significant delays in the deployment of public safety broadband networks and other inefficiencies.

A. The Commission Should Focus on Ensuring Nationwide Interoperability While Preserving Flexibility in Implementation.

The public safety community and industry share the Commission's goal of nationwide public safety broadband interoperability. Within an interoperability context, flexibility in broadband deployments must be provided. Commission rules must be flexible enough to allow the industry and public safety to adapt based upon their resources, needs, and experiences. Subjecting such modification to the normal multiyear rulemaking process could retard deployment, jeopardize service to public safety, and

negatively impact the public they protect. The Commission should only adopt those rules essential to establish a framework at this time, and those rules should be crafted to facilitate the ongoing evolution of public safety broadband services.

MSI supports the proposed definition of interoperability that has been developed by local and state public safety representatives through the DHS SAFECOM program.[3] In implementing that definition, interoperability should be considered from an end-user point-of-view, and should be characterized in terms of compatibility among application clients and servers, as well as functional compatibility and performance requirements that enable the required applications. Interoperable components should be specified in terms of the applications and their associated interfaces. As long as these required interfaces are implemented accordingly, the details and construction of the underlying regional deployments do not need to be specified to attain interoperability.

For the PSBN, the essential interoperable applications today are access to data, multimedia messaging, and video streaming. Additionally, Internet access and agency-specific applications are required. To support the minimum required interoperable functionality, certain standard client-device (*e.g.*, API), device-network (*e.g.*, Uu), network-network (*e.g.*, S6a, S8, S9, Billing, SMTP), and network-server (*e.g.*, SGi) interfaces must be implemented. While additional common interfaces are likely to be

---

[3] *See Fourth Notice* at ¶ 16 (proposing to adopt the Department of Homeland Security Office of Interoperability and Compatibility definition of interoperability as "the ability of public safety agencies to talk to one another via radio communications systems—to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."). MSI notes, however, that this definition and its reliance on "real-time" exchanges may be voice-centric as some data applications are not always performed in real-time. The Commission should keep this in mind when establishing interoperability standards.

included in any LTE implementation, they are not strictly necessary to interoperability, and thus should not be mandated by the Commission.

B. The Commission Should Identify the Architectural Guiding Principles of the Public Safety Broadband Network.

MSI supports the Commission's decision to identify architectural guiding principles for public safety broadband deployment. However, the Commission should limit itself to identifying only these architectural guiding principles and not attempt to codify details of the technology, functionality, and governance processes underlying the network. Only those rules essential to establish an architectural framework should be adopted at this time, and those rules should be established in such a way as to allow for the evolution that will take place as experience is gained.

To illustrate, identification of LTE as the standard technology protocol for the public safety broadband system is an appropriate guiding principle, however the Commission should take care to avoid over-specifying this requirement. LTE Release 8 has always been considered merely one iteration in an ongoing process of the evolution of the standard and associated technology development. New releases are developed with maximum care to ensure backwards compatibility in a multi-vendor vendor environment and interoperability with each prior release. Subsequent releases are completed yearly or almost yearly and incorporate new interfaces and/or functionality. For example, although LTE was first envisioned as a data transmission protocol, future releases will accommodate real-time voice communications. It is thus essential that public safety agencies operating LTE systems have the flexibility to choose, at the time of maturation for each release, the exact timing and the specific features to be deployed, according to their needs. An overly detailed mandate requiring public safety to

implement unnecessary interfaces defined in Release 8 will be in no one's best interest, particularly if protracted rule making proceedings are necessary to consider Commission revision and/or adoption of future releases.

Relatedly, the Commission should not adopt its proposal to require full and ongoing interoperability testing ("IOT") on "all LTE capabilities and functions" required.[4] The Commission should only set high-level interoperability requirements supported by testing rules that are sufficiently flexible to embrace technological evolution without a new rulemaking every time public safety needs to streamline implementations or adopt the latest 3GPP release. The Commission should require that all user devices be subject to conformance testing to ensure basic interoperability,[5] and should limit IOT for the roaming interfaces that extend across operator networks.[6] Any more detailed IOT or conformance testing requirements will add cost, delay deployment, and inhibit public safety network operator flexibility without any real gain in terms of inter-network interoperability.

To accommodate the necessary flexibility, it is reasonable to codify common characteristics as guiding principles rather than detailed mandates. The Commission should focus on identifying "what" needs to be implemented, rather than "how" and/or "when" to implement. Furthermore, in articulating guiding principles, it is appropriate for the Commission to provide non-mandatory, non-exclusive illustrative examples through the "such as" construction, at it has done in the *Fourth Notice* with respect to its

---

4 *See* Fourth Notice at ¶ 114.

5 *Id.* at ¶ 106.

6 These interfaces are: S6a – between MME and HSS, S8 – between SGW and PGW, and S9 – between Home PCRF and Visited PCRF.

proposal to require the support of roaming capabilities "such as Home-Routed and Local-Breakout."[7] As discussed in more detail in the attached Technical Appendix, these two roaming configurations are appropriate under different circumstances and requiring all networks to support both home-routed and local breakout roaming is excessive, burdensome and inefficient. Similarly, different network implementations will benefit from different sets of applications. For these reasons, it is appropriate that the roaming configurations continue to be illustrated by example only and not more detailed mandates.

Complicating the effort to precisely specify which applications and features should be incorporated into the PSBN is that some of the applications and features discussed in the *Fourth Notice* are not yet standardized or ready for widespread deployment. For example, supporting LTE Voice communications should be a long-term goal of every public safety broadband network. However, LTE network technology and roaming support for VoIP communications is nascent and still evolving. Another example is Category 1 handover, which is not defined in 3GPP specifications, and the implied functionality is not typically implemented in commercial networks. Mandating the implementation of such features is premature and could add unnecessary costs and delays for public safety deployments. More work is needed to define and characterize interoperable applications.

Development of the architectural framework and guiding principles should be conducted in collaboration with representatives of public safety and the technology

---

[7] *See, e.g.*, Notice ¶ 19 (proposing as a common characteristic of regional or tribal networks the support of roaming capabilities "such as Home-Routed and Local-Breakout").

community. To supplement the guiding principles suggested by the Commission in the *Fourth Notice,* MSI respectfully offers the following additional suggestions for inclusion as guiding principles:

1. Regional and tribal network deployments can define their own Access Point Names (APN's) and local routing for local applications.
2. Regional and tribal network deployments can define local QoS policies and deploy local Policy and Charging Rules Functions (PCRF) for control of their application data networks.
3. Regional and tribal network deployments can deploy their own local Packet Data Network Gateways (PGWs) and Serving Gateways (SGW) to limit transport costs for their local applications.
4. A national QoS framework should be developed, which includes specifications for nationwide Allocation and Retention Prioity (ARP) and QoS Class Identifier (QCI) usage.
5. Regional and tribal network deployments can have direct Home Subscriber Server (HSS) access to add/change/delete subscriptions for their users in real-time.
6. Regional and tribal network deployments can have direct HSS access to modify subscription parameters for their users in real-time.
7. A national IP numbering plan should be developed, such that regional/tribal network deployments can plan to interconnect with a national IP backbone.
8. A national PLMN ID framework should be developed, which includes numbering plans and guidelines for numbering LTE components and resources.

Through the adoption of these or similar proposed guiding principles, the Commission can preserve appropriate local control over public safety broadband operations consistent with the requirement of nationwide interoperability.

Upon establishing an architectural framework, an organization needs to be empowered with the responsibility for defining the more discrete implementation requirements and managing the technologies and interfaces of the network going forward. Instead of codifying the technical details of public safety broadband network engineering into its rules, this organization should work with all concerned stakeholders to make recommendations and develop best practices on an ongoing basis. The organization must

be representative and responsive to the operators of the tribal and regional networks as well as the end users. This entity must have the expertise to monitor technological advances and coordinate the management of multiple regional network evolutions. Most importantly, the organization must be sufficiently nimble to respond to fast moving technological changes that will improve public safety communications capabilities.

III. THE COMMISSION SHOULD ENSURE THAT THE PUBLIC SAFETY BROADBAND NETWORK ARCHITECTURE AND GOVERNANCE STRUCTURES DO NOT ADD COST OR DELAY TO BROADBAND DEPLOYMENT.

In light of the Commission decision in the *Third Report and Order* to defer further consideration from the public-private partnership/network sharing agreement model, it has become necessary to reexamine basic notions about how the nationwide interoperable public safety broadband network will be deployed, managed, and funded. MSI supports the vision of a nationwide network comprised of interoperable, regional or tribal all-IP LTE network deployments operating in the public safety broadband spectrum. As discussed above, regional and tribal public safety operators must be allowed to provide enhanced applications or features on top of those needed for nationwide interoperability. A nationwide IP backbone network should be available, but its use should not be required to operate the regional network deployments, and its use should not be mandated. Use of private and commercial IP backbone solutions should be allowed to promote competitive pricing and leverage technological innovations, as long as interoperability is maintained. Similarly, additional network and service platforms should be available at the national level, but remain optional for regional network deployment usage.

Various models for governance of the nationwide interoperable public safety broadband network are conceivable. These alternatives could vary in terms of the level of national control and coordination exercised and the legal status of the entity or entities exercising this control. While various approaches may have advantages and disadvantages, MSI believes that consideration must be given to how quickly such a structure or entity could be established and operational, so as not to delay current and future broadband deployments. Similarly, consideration must be given to the cost of formulating and maintaining any such entity or adding functions to existing organizations or entities. To the extent that existing structures and competencies can be leveraged to accomplish successful governance of the public safety broadband network, this will save both time and money.

One approach might be to allow state governments (working closely with relevant state and local public safety entities) to oversee public safety broadband activities within their area. MSI is aware that some public safety organizations have also suggested the formation of a federally-funded quasi-government entity comprised of public safety representatives to handle governance for the nationwide network. The *Fourth Notice* also asks about the extent to which the Commission should perform these functions.

Each of these approaches strikes a different balance between top-down mandated, centrally-coordinated decision-making on the one hand and bottom-up, local control and market competition on the other. Whichever approach is utilized will require identification of a secure source of funding both to support the administrative operations of the selected governance body, and to perform the construction of the network itself. As indicated throughout these comments, MSI believes that the best alternative is one

that emphasizes regional, tribal, and local control over the planning and oversight of broadband deployment, while delivering nationwide interoperability. Motorola Solutions recommends that the body include broad state and local government and public safety as well as industry representation in the decision-making process.

There is a clear and practical need to manage the public safety broadband network deployments at a regional rather than a national level. While the need to ensure nationwide interoperability is essential, the underlying technology evolves on shorter timescales than national-level policy creation and regulatory rule-making can accommodate. From a longer-term perspective, it could be possible to review and approve high-level regional plans on the timescales that would be expected from a federally-managed national-level policy body. However, it is imperative to allow regions sufficient flexibility on shorter-term timescales to manage technology evolution while ensuring compliance with the nationwide interoperability framework. This approach also fuels competition among vendors to provide innovative solutions to the regional and tribal networks, while staying within an interoperable framework.

Another potential governance model to accomplish these goals would be the establishment of an organization with a small number of organizational "layers" that would be made up of representatives from public safety, industry, and government. Public safety representatives should comprise the head of such an organization, which would be responsible for setting the mission, goals, and objectives, and for interfacing with National government authorities. Sub-layers must be constituted with sufficient representation by all regions of the Country as well as all facets of the public safety community. The majority of the operating and deployment decisions should be made at

the local level, close to those who understand the respective needs of the region, while still meeting nationwide interoperability requirements.

A more decentralized organization would allow the distribution of authority to the appropriate regional and local levels to adopt technical advances based on need and implementation ability, while also maintaining interoperability consistent with the architectural guiding principles. The guiding principles, as discussed above, would be determined by the Commission or some other appropriate body with input by the highest levels of the governance structure. Regional, tribal, and local authorities would ensure that the guiding principles are being fully implemented. Local/Regional public safety officials are the ones with accountability to the public they serve. A regional broadband deployment must be designed to meet local needs in conjunction with nationwide interoperability requirements to provide the requisite level of service to the public.

A successful governance and implementation process should also benefit from the involvement of appropriate third parties. Industry and technical groups should be involved, both as participants in and as service providers to the governance structure. Private sector involvement will be particularly crucial, as LTE is conceived of as an evolutionary process and it will be necessary for long term network planning to be informed by first-hand knowledge about the ongoing technology development processes.

IV. NATIONWIDE ROAMING IS ESSENTIAL TO THE SUCCESS OF THE PUBLIC SAFETY BROADBAND NETWORK.

MSI agrees with the Commission's conclusion that 700 MHz public safety broadband users should be able to roam across all 700 MHz public safety broadband network deployments and that regional public safety system operators should have an obligation to enter into roaming or other mobility arrangements on reasonable terms and

conditions to ensure this result. However, it is not necessary for the Commission to promulgate a standard roaming agreement. Because the available capacity and prioritization to support roaming could vary, we expect there would need to be some local/regional input to any roaming agreement. Public safety entities should be afforded the latitude to select and modify roaming agreements based on their needs and benefit from competition in the market. Also, under the nationwide network approach being discussed as an alternative, the movement of public safety users across the country may not require roaming agreements *per se*. Regardless of the regulatory mechanism that is ultimately implemented, it is important that access and prioritization on a local/regional system by a visiting public safety user be under the control of the local public safety system operator. As stated in the Commission's proposed definition of interoperability, communications should be "as needed and as authorized."

While it is unnecessary for the Commission to mandate a specific roaming configuration in its rules, whichever body is ultimately responsible for crafting the details of the nationwide architectural framework should recognize home-routed roaming as the preferred general-purpose roaming configuration that will support most of the applications required on the public safety broadband network. Unlike home-routed roaming, local-breakout roaming is a special purpose configuration designed to minimize bearer path latencies for certain applications. Local-breakout roaming requires increased coordination and specification in the roaming agreements between roaming partners, including support for identical applications hosted in a separate data networks. Local-breakout is an advanced capability which is not necessary for basic interoperability, and

because of key security concerns and other complexities, it should only be recognized as an optional configuration.

Each region should have the ability to specify the prioritization of users within their region based on regional criteria. However, admission of different categories of public safety roamers on the visited network should be provided consistent with a national QoS framework. While regional operators must be empowered to specify priority levels with the region, interoperability can be maintained through the mapping of home-determined priorities as visiting users roam into a region.

Finally, any roaming service charges or charging functions should not be regulated by the Commission. Unlike with commercial carriers, it is anticipated that revenue generation will not be a significant driver for implementing public safety roaming. Instead, roaming will be implemented to better protect the safety of citizens, and as a result, roaming service reciprocity will likely be extended to adjacent regional networks to facilitate mutual aid. Under this scenario, there is likely to be little incentive for public safety network operators to charge each other for roaming access.

V. FEDERAL ACCESS TO THE PSBN SHOULD BE ENCOURAGED.

Public safety incidents of any level often require coordination among state and local agencies and Federal officials. Clearly, the public interest is served by providing for routine mechanisms that authorize Federal use of the PSBN.

Under the previously adopted regulatory framework, the public safety broadband licensee had the sole authority to permit Federal users access to the 700 MHz public safety broadband spectrum. MSI agrees with the Commission that the scope and terms of Federal use of 700 MHz public safety broadband networks should be determined by the regional network operators in consultation with the PSBL. Local control and

management would enhance the ability to prioritize all users, including Federal officials. Therefore, any governance agreements regarding Federal use of the network should involve both the PSBL and the local/regional/tribal authorities who deploy the broadband networks in their respective area. Such agreements should also provide regulatory authorization for Federal users to gain access to networks while roaming.

VI. SECONDARY RESPONDERS SHOULD BE PERMITTED TO USE THE NETWORK.

From a policy perspective, MSI supports providing public safety organizations the ability to decide what entities should have access to the 700 MHz public safety spectrum. There should be no question that state and local public safety officials would ensure that the primary use of 700 MHz public safety systems would be to support the efforts of emergency responders who protect lives and property. Complementary users, such as secondary responders, utilities or other critical industries would likely be permitted only at lower priority level and only to the extent that there is adequate capacity reserved for police, fire and other emergency care providers. It is unfortunate that the literal language of Section 337 of the Communications Act has unwittingly created regulatory uncertainty in an area where an operational problem is unlikely to exist. The preferred solution would be to modify the statute so that the Commission has authority to draft rules that extend decision-making responsibilities on eligibility to the local level.

Until that occurs, however, the Commission and public safety organizations must comply with the existing law. The Commission has previously made clear that state and local governmental agencies are eligible to secure 700 MHz narrowband licenses without

a further showing of eligibility.[8] MSI sees no need for the Commission to deviate from this prior interpretation of the statute, recognizing that the applicable issue here is eligibility, not licensing, because the public safety broadband spectrum is licensed to one entity on a nationwide basis. Indeed, to the best of MSI's knowledge, no party has challenged this previous Commission interpretation. Section 337's requirement that use of the network must be "to protect the safety of life, health, or property" appropriately embraces secondary responders associated with city or governmental related organizations that serve the needs of the public. The Commission should be confident that local authorities will limit access to those entities that will use the network in an efficient manner and to prioritize that access appropriately given the scarcity and value of the 700 MHz spectrum.

VII. RELOCATION COSTS FOR INCUMBENT NARROWBAND SYSTEMS SHOULD BE COVERED AS A COST OF BROADBAND DEPLOYMENT.

In creating a consolidated public safety broadband allotment in the 700 MHz band, certain narrowband operations are stranded on frequencies no longer available for that technology except through waivers to continue operations, pending relocation to comply with the revised plan.[9] In order to achieve the goal of a nationwide public safety broadband network, the narrowband incumbents must be relocated.

---

[8] *See* Development of Operational, Technical and Spectrum Requirements For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, *First Report and Order and Third Notice of Proposed Rulemaking*, WT Docket No. 96-86 (rel. September 29, 1998); and Development of Operational, Technical and Spectrum Requirements For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, *Second Memorandum Opinion and Order*, WT Docket No. 96-86 (rel. August 1, 2000).

[9] *See Implementing a Nationwide, Broadband Interoperable Public Safety Network in the 700 MHz Band,* Second Report and Order, 22 FCC Rcd 15289 (2007).

In its Order granting conditional waivers to 21 public safety petitioners to deploy broadband networks, the Commission required waiver recipients to protect 700 MHz narrowband incumbent operations through appropriate engineering measures or geographic exclusion, or to relocate them at their own expense.[10] These actions were made subject to further consideration of relocation issues in this proceeding, and the Commission declined at that time to address the costs for such relocation or any potential reimbursement.

It is clear that, at least for the foreseeable future, public safety has a need for both narrowband and broadband 700 MHz band operations. The pivotal issue in resolving the narrowband relocation issue relates to the availability of funding and the process to obtain those funds. Various bills have been introduced in Congress which include funding for public safety broadband deployment. MSI believes that the costs of relocating the narrowband systems to comply with the revised bandplan should be included as an eligible expense as part of the costs to deploy broadband systems.

In general, narrowband 700 MHz licensees who began their system deployment after the Commission's decision to revise the bandplan do not need to be relocated, as they already operate in accordance with the new bandplan. It is only those public safety entities that began deployment prior to the band plan revision who would need to be relocated. Therefore, the scope of the relocation is somewhat limited and not every current or pending broadband waiver grantee will face the issue of relocating narrowband systems. Licensees who still need to be relocated will need to have their costs funded as

---

[10] *Waiver Order*, 25 FCC Rcd at 5168, ¶¶ 72-73.

part of any broadband deployment that would otherwise interfere with continued narrowband systems still operating under the previous bandplan.

In this regard, MSI believes that all narrowband relocation costs for such licensees should be covered. The Commission's previous proposal in the 3rd FNPRM included reimbursement of "hard" costs and none for "soft" costs, but did not clearly delineate what falls into each of these categories. As noted in the previous Motorola, Inc. comments to that 3rd FNPRM:

> The Commission should clarify that all costs necessary for relocation and rebanding projects must be reimbursed. For example, equipment (including software) is clearly a "hard cost" and would be reimbursed. The Commission should make clear, however, that any labor necessary to produce or modify the equipment should also be reimbursed. In addition, services provided in direct support of a frequency relocation project, including project engineering, project management, and technician support, should likewise be reimbursed. Whether or not such services would be deemed "soft costs," they should be equally eligible for reimbursement because they are required to perform a relocation project.[11]

Because legitimate relocation costs vary widely by equipment and agency, a complete and accurate estimate of relocation costs can only be created by soliciting information on those costs directly from individual public safety agencies affected by 700 MHz band relocation. MSI believes the relocation cost issue can be handled most fairly by requiring affected narrowband 700 MHz licensees to submit detailed relocation plans and not-to-exceed cost estimates just prior to the start of the relocation and within whatever process provides the funding for the relocations.

The Commission asks questions in the *Fourth Notice* regarding the process and timing for any consent between narrowband 700 MHz licensees who must relocate to the

---

[11] Comments of Motorola, Inc., WT Docket No.06-150, submitted Nov. 3rd, 2008, at 22.

revised narrowband portion of the bandplan to make way for broadband deployment. MSI believes that the timing and requirements should be linked to broadband deployment funding process. Setting yet another set of logistic requirements without having certainty on the actual source of relocation funding merely creates additional work for public safety narrowband licensees that in all likelihood would need to be redone.

VIII. CONCLUSION.

The establishment of a nationwide wireless broadband network that provides interoperable access to first responders is long overdue. MSI pledges its resources and expertise to helping the Commission and the public safety community develop an appropriate technological and governance framework that best meets the needs of end users. With the right regulatory flexibility and governance structure, both nationwide interoperability and local control will be achieved. Users must be able to access the network as needed and as authorized wherever they are located; the need for local/regional design and operational control to meet the accountability of the public that public safety officials and responders serve is equally important. The rules and governance should also foster innovation and competition in the delivery of equipment and services so that public safety users continue to have access to the best technology and solutions available.

Respectfully submitted,

/s/ Chuck Powers
Chuck Powers
Director,
Engineering and Technology Policy
Motorola Solutions, Inc.
1455 Pennsylvania Avenue, N.W.
Washington, DC 20004
(202) 371-6900

April 11, 2011

Technical Appendix:

Further Analysis of the Third Report and Order and Fourth Further Notice of Proposed Rulemaking

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

Technical Appendix

Further Analysis of the Third Report and Order and Fourth Further Notice of Proposed Rulemaking

I. INTRODUCTION

In this Technical Appendix, Motorola Solutions, Inc. ("MSI") supplements its initial comments with additional feedback and analysis on the technical proposals contained in the Federal Communications Commission's Third Report and Order and Fourth Further Notice of Proposed Further Notice of Proposed Rulemaking related to the establishment of a nationwide interoperable public safety broadband network.[1] As MSI explained in its Comments, the Commission should not adopt rules pertaining to the discrete technical details of public safety broadband network design and deployment. Rather, the Commission should identify the architectural framework and guiding principles to ensure interoperability, while enabling regional, local, and tribal public safety entities to exercise control over the characteristics and specifications of their networks. Nevertheless, in the interest of informing the Commission's decision-making processes, MSI herein responds in detail to many of the proposals and questions contained in the Notice. To be clear, however, MSI's comments below are meant purely as background and as recommendations for future best practices development, unless expressly indicated otherwise.

II. COMMENTS ON THE THIRD REPORT AND ORDER

MSI supports the Commission's determination that LTE should form the common technology platform for the nationwide public safety broadband network. However, several of the related decisions the Commission made concerning the details of LTE implementation could ultimately hinder broadband deployment. For example, it is unnecessary to require that any releases after LTE Release 8 that are implemented in the public safety broadband network ensure backwards compatibility with all other LTE releases because similar objectives are considered in LTE and the 3GPP standardization processes. Adopting this requirement simply adds confusion without a concomitant benefit. With the understanding that networks will need to be upgraded periodically as technology evolves, deploying 3GPP standards-based systems provides as much "future proofing" as reasonably possible.

Similarly, the long list of LTE interfaces for which the Commission has mandated public safety broadband networks demonstrate support from day one do not all equally promote interoperability and are likely to unnecessarily delay delivery of crucial public safety communications services.[2] While almost all of the LTE Release 8 interfaces that the Commission has identified as being necessary will provide needed capabilities for public safety, several of the interfaces intended to enable roaming and handover capabilities do not need to be fully supported until certain additional technical or deployment milestones have been achieved.

---

[1] *See* Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, *et al.*, WT Docket No. 06-150, PS Docket No. 06-229, WP Docket No. 07-100, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 26 FCC Rcd 733 (2011) ("Fourth Notice").

[2] Fourth Notice at ¶ 12.

For example, it is premature to require support for the S8 and S9 interfaces until after a minimum number of in-service networks have been deployed to enable viable roaming partner opportunities. These interfaces, each supporting different roaming services, would require not only roaming partners (*e.g.*, other networks on which to roam), but also the support of a roaming service provider to enable the necessary interconnections, with the associated roaming fees. During the initial roll out of these networks, the small number of broadband networks that are deployed would not provide enough roaming opportunities to warrant the cost of deployment. Once multiple networks are in service, these interfaces can be easily implemented as an upgrade, without decommissioning or replacing already deployed equipment.

Similarly, it is reasonable to require the S10 interface itself upon achieving service availability. However, the additional requirement to support Category 1 handover should be separated from the basic S10 requirement. Category 1 handover is not a 3GPP specification, but is instead a concept briefly described in the NPSTC BBTF Technical Report as handovers between Home and Visited Public Safety LTE networks.[3] Support of Category 1 handovers should not be required until an industry consensus specification for this type of handover has been developed.

Finally, the requirement for the Gy and Gz interfaces should be addressed separately, as they support online and offline charging, respectively. Offline charging information managed via the Gz interface does not affect, in real time, the services rendered. As such, this is similar to existing public safety charging mechanisms, and may be appropriate for initial LTE deployments. However, online charging, as defined in the Gy interface, is a model that requires real-time credit authorization for network use (among other functions), which is not a billing model that is applicable to public safety networks. Therefore, we believe support for the Gy interface should not be required of all public safety broadband deployments.

III. COMMENTS ON THE FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING

MSI's overarching views on the Fourth Notice are presented above, in the main body of its comments. Below, MSI provides additional technical detail in response to the numerous questions posed by the Commission in the Fourth Notice. The structure of these responses generally tracks that of the Fourth Notice, and the specific paragraphs being responded to are indicated at the top of each subsection.

A. Technical Rules for the Public Safety Broadband Network

Rather than attempting to codify aspects of the design and management of the public safety broadband network, the Commission should instead focus on identifying the basic requirements for interoperability and otherwise provide sufficient flexibility to public safety to develop broadband networks that are responsive to their needs and capable of adapting to evolutions in technology while also providing interoperability.

---

[3] *See* Public Safety Spectrum Trust Ex Parte Filing, PS Docket 06-229 (Dec. 15, 2009) (entering into the docket National Public Safety Telecommunications Council, 700 MHz Public Safety Broadband Task Force Report and Recommendations (2009).

1. Architectural Framework (response to paragraph 17)

The guiding principles should facilitate network and service evolution from technological, operational, and capital expenditure perspectives. As such, the principles should focus on higher-level interoperability goals and objectives. As discussed below, the Commission should adopt some, but not all of its proposed guiding principles.

2. Architectural Guiding Principles (response to paragraphs 18-25)

Components of the Nationwide Network. The Commission must clearly identify what functions and services are to be provided by the nationwide/national elements, as well as which organizational and/or governmental entities will be responsible for funding, creating, operating, and maintaining these elements.

Regional or Tribal Network Characteristics. Establishment of an architectural framework should be conducted in partnership with public safety practitioners and equipment vendors. An independent, collaborative organization may be better suited to establish and maintain a framework that defines and manages these implementation requirements, allows significant representation from the practitioner community, and may have more latitude to adjust and update the framework more frequently and with more granularity based on practitioner feedback.

Home-routed and local breakout roaming configurations are useful for specific network applications, but are not useful for all network applications. Therefore, requiring that all networks support both home-routed and local breakout is excessive, burdensome, and inefficient. Further, the baseline applications are not well defined, and thus requiring they be supported is not warranted. In addition, application usage of local breakout roaming has not been identified. There are several issues associated with local breakout, such as inter-domain security enforcement in the UE (devices), and home network policy implementation and monitoring for internet access. For these reasons the usage of local breakout should be referenced by example only.

Roaming Authentication and Internetworking Functions – Clearing House. Regarding LTE/EPC and IMS networks, according to 3GPP standards, roamers are authenticated by their home network, and not by the visited network. Therefore, a clearing house is not involved in authenticating roamers for LTE/EPC or IMS services. However, an IPX roaming service provider may provide DIAMETER routing agent (DRA) and Domain Name Service (DNS) functions to support inter-domain transport of authentication signaling messages.

Authentication for non-IMS applications is not addressed in 3GPP standards. Therefore, non-IMS public safety data applications may benefit from a centralized authentication service, which can serve as a generic trust-bridge. It is possible that "clearing house" organizations could support such authentication services for non-IMS applications. However, given the varied requirements for these applications, efficient and effective codification of this principle would be difficult to achieve.

The term "clearing house" in the Fourth Notice requires clarification. Clearing house services generally do not include IPX transport services. There are two types of roaming clearing

house services: data clearing and financial clearing. Data clearing services provide data usage information exchange services via Transferred Accounts Procedure (TAP) and Returns Accounting Process (RAP) records. Financial clearing services provide financial settlements. Roaming hub services provide bearer traffic transport, eg, using the IPX specification, however these are not typically considered as "clearing house" services. Commercial providers can be leveraged for each of these services on a nationwide basis. Alternatively, a national IP transport backbone could provide bearer traffic transport, e.g., using the IPX specification and associated security and DIAMETER routing services. However, the national IP transport backbone would need to offer comparable or better security, quality, and availability as commercial service providers can offer, yet at a lower overall cost to public safety operators.

Nationwide Services and Capabilities. Industry usage of the term "clearing houses" typically does not include authentication services or directory services. However, it is reasonable to consider that application-level authentication and/or directory (eg, DNS) services could be provided on a nationwide basis. In this context, third party organizations or a national organization could be created to provide these services. However, the national application-level authentication and/or directory services would need to offer comparable or better security, quality, and availability as commercial service providers can offer, yet at a lower overall cost to public safety operators.

Evolution. LTE Release 8 represents an evolution of a prior and well developed 3GPP system (UMTS). As a consequence, it is technically solid and captures essential functionality to support nationally and internationally deployed networks which can interoperate. There have been surprisingly few technical problems identified in Release 8 that required actual change to the specifications. The development of specifications in 3GPP is mindful of the documented processes, while rules tend to be enforced strictly by the 3GPP Secretariat. In general, releases are developed with maximum care to guarantee backwards compatibility in the framework of coexistence of multi-vendor equipment compliant with various LTE releases. Releases subsequent to Rel-8 are completed yearly or almost yearly and they bring in new functionality. Although the first envisioned uses for LTE were for data, today the standard has matured to the point where later LTE releases will accommodate real time voice. It is thus essential that public safety agencies operating LTE systems have the flexibility to choose, at the time of maturation for each release, the exact timing and the specific features to be deployed, according to their needs.

We also note that resolution of the PLMN ID allocation issue may impact the scope and type of network sharing opportunities, and as such, timely resolution of this issue is critical.

Sharing core network resources could reduce overall costs in a carefully planned and coordinated network. Elements of a shared network may include an IP transport backbone, a DIAMETER routing network, and a centralized billing system. However, doing so requires funding to design and implement the network. The technical aspects of sharing network resources should not be overlooked in planning the organizational structure. Moreover, recognizing that all of this will take time, the Commission should be cognizant that, because of operational needs and/or requirements imposed by funding sources, some public safety entities will need broadband solutions in advance of rulemaking efforts in this docket being concluded.

Individual public safety entities cannot be expected to sit idle while the rulemaking process is completed months (or more) down the road.

3. Open Standards (response to paragraphs 27-28)

Open standards enable vendors to build to a common reference architecture and associated interfaces for interoperability and are carefully balanced to enable innovation within the framework of the standards. Such latitude is essential to foster competition in open markets. As such, open standards provide a reference architecture, a "tool box" of capabilities, and a functional foundation from which to implement market-specific product features. Useful technologies may not be patented for several reasons, such as narrow application, prior disclosure in the public-domain (*i.e.*, lack of novelty), and insufficient business justification (*e.g.*, return on investment) to pursue obtaining a patent.

It is important to establish *baseline* operations that must be met to achieve interoperability. As the name implies, baseline operations include only absolute minimum requirements for functionality and do not prevent or exclude subsequent inclusion of other capabilities or interfaces. For example, devices must be able to obtain service by attaching and establishing default bearers across public safety broadband networks. Beyond that additional impacts should be assessed based on further definition of the scope and objectives of nationwide interoperability.

We recommend these baseline operations be comprised of attaching and establishing default bearers in a visited public safety 700 MHz broadband LTE network. Some public safety operators and their users may require additional functionality, beyond the baseline functionality. However, this additional functionality will not be required (or desired) in all public safety networks. Therefore, additional functionality, beyond the baseline, should initially be considered out-of-scope with respect to interoperability requirements, but should not be constrained.

Also, the Commission asked about proprietary features. As noted previously, Motorola fully supports the LTE standard. To the extent that some users require features that are technically viable but not yet standardized, allowing such features to be deployed helps meet public safety requirements and promotes greater competition among vendors.

4. Technology Platform and System Interfaces (response to paragraphs 29-31)

The Third Report and Order contains a comprehensive list of 3GPP defined interfaces \ identified by the Commission as being required for public safety. However, not all of those interfaces are required for public safety interoperability. See comments in Section II, above, regarding the S10 and Gy interfaces. As the specifications evolve within the 3GPP organization through successive releases, new interfaces are being defined. Some of those interfaces may become useful to public safety applications, while others may just support functionality that is outside the sphere of interests for public safety.

While 3GPP issues new releases of its specifications with some frequency, their mandatory adoption by the public safety community should be subject to a determination of not

only their suitability to the tasks at hand, but also of the maturity level of both the specifications and the availability of compliant products.

The rules under which 3GPP operates require that newer releases stay backward compatible with previous releases. During operations, many interfaces include information obtained via signaling and/or from configuration databases assure that all subsystems are capable of identifying the release level of other subsystems. Therefore, one can say that compatible interoperability is reasonably built into the LTE platforms.

Releases 9 and 10 of LTE contain some important features that may be of interest to public safety. Those include, among others, broadcast multicast service (MBMS), control plane location services, and relays.

However, before those new capabilities are adopted for public safety, certain criteria should be met. First and foremost, there has to be a good functional fit. Beyond that, though, several determinations will need to be made that the selected capability is mature enough in both specifications and implementations, that deploying it represents a best use of spectrum and other resources (including financial resources) in comparison to other possible solutions and that enough testing and/or commercial use has occurred for a reasonable expectation of reliability of the services and devices. Therefore, it is recommended that some studies, specific to each capability, be performed before issuing regulations mandating support of the particular capability arising from LTE Release 9 and higher.

As already mentioned, the specifications development process in 3GPP ensures backward compatibility between communicating subsystems. In addition, configuration profiles in various databases combined with the ability of systems to handle errors gracefully provide an additional layer of protection and interworking. Therefore, synchronizing LTE release across disparate networks is not strictly necessary, as the integrity of those systems is not endangered by communications with systems using older or newer releases. In this way, the rather difficult and risky task of trying to simultaneously roll out the same release within multiple networks can be avoided.

Although LTE has been designed to support voice, the first generation of applications and user devices are data oriented. It is thus to be expected that public safety deployments will initially provide data over LTE. This will coexist with voice services provided by legacy systems (e.g. P.25 compliant) and may interwork via gateways to provide universal access. It is important that voice services over LTE are first determined to be reliable before being mandated.

The technical and operational challenges of deploying a nationwide system of this complexity over a short period of time should not be underestimated. It is thus recommended that the diverse needs and means of the many jurisdictions and agencies that make up the public safety community be recognized through a regulatory framework that sets a firm and clear technical direction, but allows maximum local autonomy and deployment flexibility, without artificially short deadlines.

IPv6 is not backwards-compatible with IPv4. Users with IPv4 addresses will not be able to access IPv6 services or communicate with IPv6 host, and vice versa, without the support of

the appropriate transitions mechanisms. These transition mechanisms, including dual-stack implementations, tunneling and translation, allow existing IPv4 systems to co-exist and interoperate with IPv6 systems.

MSI does not recommend requiring the entire network to be IPv6-based from day one. It is possible to implement an IPv6-based transport backbone to enable nation-wide reachability among the core-network equipments from day one. However, the transition from IPv4 to IPv6 for end user traffic will likely take a significant amount of time due to the need to support, and ultimately migrate, legacy systems and services that are currently IPv4-based.

In paragraph 30 of the Notice, the Commission inquires as to the benefits and challenges of launching an all IPv6 network:

Benefits:

- Significantly larger address space
- Build-in Security (IPSec at network layer) enables ubiquitous security services for end-to-send network communication
- Seamless and Simplified routing
  - IPv6 allows more optimal routing for mobile users as IPv6 mobility specification are designed to eliminate "triangular routing".
- Facilitate end-to-end services and applications by eliminating the need for NAT
  - Enables push-applications and peer-to-peer based applications
- Reduce network management/administration cost
  - IPv6 provides auto-configuration capabilities. Hence, networks are simpler, flatter and easier to manage.
  - Removal of NAT equipment simplifies the network
- Possibility of improved QoS (enabled by "flow label" field in the IPv6 header)
  - Further study is needed to fully define how to take advantage of flow labels.

It should be noted that not all the benefits mentioned above can be realized during the transition period in which both IPv4 and IPv6 networks co-exist (See Challenges below).

Challenges:

- IPv6 is not backwards-compatible with IPv4. The IPv6 and IPv4 protocol cannot intercommunicate without transition mechanism (dual stack, tunneling or translation). Although theoretically IPv6 may reduce network management/administration cost in the long run, the total operational expenses during transition period will likely to increase rather than decrease.
- Most government agencies deploying public safety LTE will have existing IPv4-based equipments and applications in narrowband system. Such agencies are not likely to be able to disrupt delivery of mission critical services over the existing

IPv4 network. There will be an extended migration period where these agencies have to support the legacy IPv4 services.

- As of today, nearly all public safety agency applications are IPv4-based. Launching end-to-end IPv6 network will significantly limit the re-use of existing state/local public safety applications.
- Possibility of interrupted service as result of roaming and mobility into IPv4-based network. The seamless mobility benefit of IPv6 deployment only applies if/when all networks are updated to support IPv6.

Similarly, the Commission also asks about the key advantages and disadvantages of having certain core network elements with IPv4 (capable of upgrading to IPv6 in future) while the rest of the network is based on IPv6.

Advantages:

- Most government agencies deploying public safety LTE will have existing IPv4-based equipments and applications in narrowband system. Maintaining IPv4 support in certain network elements (at least during the migration period) maybe necessary to avoid disruption to delivery of mission critical services over the existing IPv4 network.
- As of today, nearly all public safety agency applications are IPv4-based. Maintaining IPv4 application servers allows re-use of existing state/local public safety applications.
- Reduce or postpone realization of cost for implementing IPv6 and/or transition mechanism.
    - Maintaining certain network elements to be IPv4-based for sometime may allow stakeholders to upgrade to IPv6 as part of normal equipment upgrade cycle – hence reduce the cost of migration to IPv6.

Disadvantages:

- Maintaining IPv4 infrastructure and services may provide acceptable level of services and functionality to most users. Hence, it may slow the rate of migration to IPv6.
- With the last blocks of IPv4 addresses were allocated in early February 2011, the clock is ticking for IPv4 exhaustion especially with the increasing number mobile phones/devices and smart appliances.
- Possibility for machine-to-machine application capability may be limited.
- IPv4 addresses cannot communicate with IPv6 addresses without transition mechanism (dual stack, tunneling or translation). Without deploying appropriate transition mechanism:
    - IPv4 servers may not be reachable by IPv6-only devices.
    - IPv6-only devices may not be able to access IPv4 servers.

- The use of NAT in IPv4 network may limit end-to-end services and applications.
- High network management/administration cost
  - Complication due to NAT equipment
  - High cost associated with network re-configuration

Although there has been increasing sense of urgency to start moving towards IPv6, there is no clear date by which end-to-end IPv6 transition is required. The benefits of IPv6 (such as removal of NAT, improved QoS) on real time application such as voice and/video cannot be realized until both client and server are IPv6 capable. If there is a mismatch of supported IP version between the client and the server, application layer translation is necessary to provide interoperability. Performance may be critical for real-time voice/video applications. Application layer translation provides application-specific translation which is necessary when the application protocol contains IP addresses. Application layer translation introduces undesirable additional processing delay for real-time applications. It is recommended that application servers are upgraded to be dual stack during the migration period where IPv4-only devices, IPv6-only devices and dual-stack devices can co-exist.

The Commission also seeks comment on dual-stack. Dual-stack deployment enables transition to IPv6 without disruption to IPv4-only devices and services. Without comprehensive testing of different applications (that exist and widely used today), an IPv6 only access would be too risky. Dual-stack transition mechanism is more appropriate in the early phase of migration to IPv6 as it allows both IPv4 and IPv6 to co-exist in the (dual-stack) devices and networks. Requiring all new devices to support dual-stack is desirable in providing a flexible operational environment for transitioning to IPv6 and to reduce capital cost. However, the main benefit of IPv6 cannot be realized until the networks and/or the applications are IPv6 ready. Also, dual-stack devices still require IPv4 addresses and as such do not mitigate the IPV4 address exhaustion problem.

Instead of requiring all new devices to be dual-stack from day one, MSI recommends that all new devices be dual-stack ready. When the system and/or the applications are IPv6 ready, upgrading these devices to support IPv6 would only require software or firmware upgrades, and no changes to hardware or physical components.

With respect to requiring network elements to support dual stack, MSI believes that this decision should be made on a case-by-case basis.

Where it is determined that IPv6 migration is needed, the following are elements which logically should be upgraded to dual stack in early phase of IPv6 migration:

- **Perimeter Firewall**: Update policies and access control lists.
- **Network Elements providing external IPv6 connectivity**: to provide IPv6-based connectivity to public-facing servers; in some cases, this includes enabling transition mechanism (such as tunneling over IPv4 cloud to another IPv6 network).

- **DNS**: DNS is used to map hostname to IP address. Since dual stack nodes are capable of communicating with both IPv4 and IPv6 nodes, the DNS must be capable of handling both IPv4 "A" records as well as IPv6 "AAAA" records associated with the dual stack node. DNS may return only "A" record (if IPv4 preference is indicated by the application), only "AAAA" record (if IPv6 preference is indicated by the application), or both types of records (if no preference is indicated).
- **Access Network, DHCPv6 Server, NTPv6 Server**: The goal here is to provide IPv6 connectivity to IPv6-capable devices.
- ***New* Application Servers:** New application servers should be IPv6 capable.

The potential cost of a dual stack requirement would depend on the state of the existing infrastructure/network elements, the timing of the upgrade, and the extent to which IPv6 has been considered as part of the network's development strategy. There is a large potential transition cost for network access providers to support dual stack deployment. However, since IPv6 has been anticipated, new networks and applications will likely encounter lower costs associated with IPv6 implementation. Major LTE providers have already planned to support IPv6 devices and dual-stack devices, and thus these costs would be considered as part of the normal or planned upgrade of the infrastructure. Legacy networks, and applications which utilize them, will incur a much larger cost associated with transition to IPv6.

Supporting two IP stacks is also likely to increase operation expenditures.

There are a few challenges/complexity associated with the dual stack deployment:

- **Shared infrastructure and resources**: The network operator shall make sure that all network resources have enough processing power and memory (e.g. routers needed enough memory to store two routing tables, larger number of access control list, etc.) to support two different IP stacks to avoid undesired increase of processing latency. The device must have enough resources to run both protocol stacks.
- **Application Protocol preference**: Dual stack devices must choose the correct protocol to successfully access a specific service (depending on what protocol is supported by the associated application servers). Dual-stack DNS incorrectly forwarding "AAAA" records to IPv4-only device may cause failure to IPv4 application to fail.
- **Security Implication**: Dual stack deployment exposes dual stack node to security vulnerabilities associated with both IPv4 and IPv6, in addition to any new vulnerabilities resulting from unintended interactions between the two. See RFC 4942, "IPv6 Transition/Coexistence Security Considerations" for more details.

The Commission also asks about the advisability of requiring the adoption of PMIP and the Gxc interface. Implementation of the Gxc interface should not be required. Generally, public safety networks will not benefit from implementing PMIP. The PMIP protocol was standardized to facilitate interworking the EPC with non-3GPP access technologies. However, public safety generally does not own or operate non-3GPP access assets. Further, the Gxc is not a standardized

roaming interface. Therefore, there is no common use case for the Gxc interface, and thus there isn't sufficient justification to require it.

5. System Identifiers (response to paragraphs 32-34)

We wish to clarify the previous MSI proposal for the hybrid scheme as follows. The separate PLMN ID's assigned to each regional or tribal network would be actual PLMN ID's, which would comply with 3GPP standards. The single PLMN ID in the hybrid scheme would be a virtual PLMN ID, which would not correspond to any actual network, and is not supported (*i.e.*, such usage is not described) in 3GPP standards. Rather, the virtual PLMN ID would be used as a pseudonym for a consortium of networks participating in nationwide roaming among public safety networks. The purpose of the virtual PLMN ID would be to reduce the size of roaming lists that would otherwise need to be maintained in public safety UE's. As such, the virtual PLMN ID would be used only in public safety access networks, and could not be exposed to public carrier networks or to billing clearinghouses. If a hybrid PLMN ID scheme were to be adopted, since not supported in 3GPP standards, a nationwide entity would need to obtain, prescribe, and manage usage of the virtual PLMN ID for the nationwide network. Given the non-standard nature of the hybrid PLMN ID scheme, and the associated potential misinterpretation of such hybrid PLMN ID, and the requirement for a central administrative authority, adoption of this scheme should be carefully considered.

Alternatively, a single traditional PLMN ID could be instituted in support of an actual nationwide network which has shared components among regional or tribal public safety networks. There are many tradeoffs associated with adopting a single traditional PLMN ID for this purpose, rather than separate PLMN ID's for each regional or tribal network. Many tradeoffs depend on which elements are actually shared. The appropriate PLMN ID assignment scheme is inherently linked to the nationwide network architecture. As such, it is imperative that a nationwide architecture be solidified before a resolution of the PLMN ID assignment scheme. However, an essential requirement for instituting a single traditional PLMN ID for a nationwide public safety network is a centralized organization and authority responsible for planning, coordinating, and maintaining shared resources. These resources may be physical, or logical, or both. System identifiers, such as PLMN IDs, Physical Cell IDs, and Tracking Area IDs are examples of shared logical resources.

The IMSI Oversight Council (IOC) guidelines for PLMN ID assignment have been in process of being changed.[4] The current version of the guidelines is version 12. In this version, PUBLIC SAFETY entities or agents on their behalf may directly obtain PLMN ID's from the IOC. Further, GSMA membership is not required to obtain a PLMN ID. As such, support from other entities, such as NIST should not be required to obtain a PLMN ID.

6. Roaming Configurations. (response to paragraphs 35-36)

The home-routed configuration should be required as the baseline roaming capability, as this is a general-purpose configuration which can be used to support the majority of public safety applications. Local breakout (LBO) is a special-purpose configuration, designed to minimize

[4] See http://www.atis.org/ioc/_Com/Meetings/2010/2010.12.17/IOC-10-12-17-06.doc.

bearer path latencies for certain applications. LBO requires agreements among roaming partners, such that well-known LBO Access Point Names (APNs) are defined and configured in each network, for applications intended to use LBO. Further, each network is required to support identical LBO applications located in a separate and dedicated data network. LBO faces the following challenges:

- A compromised or improperly implemented device can enable data routing between security domains comprising the APN networks
- Accessing applications from the visited system bypasses home agency proxies, firewalls, and antivirus measures
- Bypasses home network logging and activity tracking

As such, LBO is an advanced capability which may be used for minimizing bearer path latencies. However, LBO is not needed for basic interoperable service. Therefore, it is sufficient to identify LBO as an optional configuration, based on deployment of applications which can use it.

Decisions regarding implementation of roaming with commercial carriers should be made by public safety operators, based on their needs and objectives.

7. Roaming Authentication and Internetworking Functions (response to paragraph 37)

The Commission should consider providing clarification of the term "clearinghouse" and its associated services. In our understanding of commonly used industry terminology, clearing house services do not include IPX transport services. There are two types of roaming clearing house services: data clearing and financial clearing. Data clearing services provide data usage information exchange services via Transferred Accounts Procedure (TAP) and Returns Accounting Process (RAP) records. Financial clearing services provide financial settlements. According to this terminology, the EPC/ LTE authentication in visited networks does not require clearinghouse services. Rather, only transport connectivity between the MME in the visited network with the HSS in the home network is required. Therefore clearing houses are not needed for EPC/LTE authentication. However, any nationwide applications may benefit from a common authentication at the application level, which could be supported by a clearinghouse. However, nationwide applications are not defined up to this Third Report and Order and Fourth Further NPRM. In this context, common clearinghouse support for authentication is not required.

8. Interconnectivity of Regional or Tribal Broadband Networks (response to paragraphs 39-42)

MSI agrees with the Commission's tentative conclusion that direct dedicated connectivity between any two regional, tribal, or local networks should not be required as there will be scenarios where the volume of traffic between them will not warrant the additional cost of dedicated links.

MSI notes that using the internet as an interconnection hub would be an unconventional approach to supporting a roaming hub. Although inexpensive, quality of service attributes such

as packet loss, latency, and delay variation could not be controlled. A lack of QoS could degrade 'real-time' applications such as VoIP and Video Streaming. Further, the source of such degradations would be difficult to isolate and remedy. Leveraging the internet for transport would not alleviate the need for DIAMETER peering points. DIAMETER peering points would be needed to fully utilize DIAMETER routing and resiliency features of the DIAMETER protocol. Internet connectivity to roaming elements requires much stronger security controls on roaming interfaces, since they would be exposed to the public internet, and therefore exposed to a wide range of attack profiles.

The term "clearinghouse" is commonly used to reference "data clearing" and "financial clearing" functions. These functions are distinct from interconnection and transport functions. The interconnection and transport functions are typically referred as "roaming transport" or "roaming hub" functions.

For the purpose of this question, we assume that clearinghouse refers to roaming transport (*e.g.*, IPX) service providers. A common roaming transport service provider is not typically required for roaming operation because the GSMA requires roaming transport service providers to interconnect with each other. One or more entities representing the public safety community may "pre-negotiate" roaming terms with one or more commercial roaming service providers and this could be helpful to some public safety entities. However, use of any pre-negotiated terms should not be mandated, as various public safety entities can have various service needs.

With respect to alternatives for interconnectivity of the regional broadband networks, MSI recommends an unregulated approach, whereby innovative and/or tailored services can sprout based on market needs and entrepreneurial ventures.

9. Prioritization and Quality of Service (response to paragraphs 43- 46)

MSI believes that there must be a nationwide QoS prioritization framework from which prioritization of public safety users is enabled across the nationwide system. The 3GPP LTE standards based attributes including access class barring, QCI, and ARP, enables a nationwide prioritization framework suitable for use of public safety responders. These LTE standards specified QoS attributes serve as a basis for enabling prioritization for public safety responders. There needs to be a public safety prioritization policy that is accepted by all regional public safety agencies, which is used across all 700MHz LTE public safety regional networks.

Support for Public Safety Priority for Network Access. MSI recommends that Access Class Barring parameters be utilized to ensure that public safety responder's can access the broadband network in extreme congestion scenarios. Higher priority access classes should be reserved for public safety first responders, whereas lower priority classes should be allocated for all other user classes.

Support for Dynamic Prioritization for Public Safety. In order to provide for dynamic QoS policy implementation, MSI recommends that the public safety broadband network should implement the LTE PCRF function. Public safety's PCRF will enable dynamic QoS policy control for responder devices, as well as enable the use of the LTE Rx interface for signaling the

needed QoS. Dynamic modification of LTE network bearers is a capability that should be implemented along with dynamic QoS policy.

Specification of QoS ARP Attributes and Preemption Capability. In order to provide prioritization for public safety responders, it is necessary that an admission control process is implemented which evaluates the requested network resources and provides admission determination using the 3GPP specified ARP parameter. For the nationwide public safety framework, standardization of the ARP value insures appropriate priority for public safety and insures LTE resources are available for critical public safety users. Defining a consistent set of ARP priority attributes across the nationwide and regional networks facilitates inter-regional system QoS, which is essential to consistent prioritization for public safety users. It is recommended that the public safety network enable preemption of bearers. Configuration of the preemption priority is based on ARP. The regional operator should configure the preemption capabilities based on regional needs for both home and visited public safety users.

Specification of QoS QCI Attributes. MSI recommends that there be standardization of the QCI values across public safety regional systems in order to provide consistency of QoS across the nationwide system. The QCI is a scalar parameter that maps to QoS scheduling characteristics at the eNB (including scheduling priority, packet delay budget, packet error loss rate, etc.). Lack of QCI standardization will result in inconsistent QoS treatment across regions in the nationwide network.

Regional Level Specification of Priority for Public Safety. MSI recommends that each region have the ability to specify the prioritization in their specific region based on their regional criteria. It is important to allow the regional operator to specify prioritization attributes within a region while accommodating prioritization for visiting users in the region. Utilization of a consistent set of ARP and QCI attributes between home and visited networks will ensure consistency for home and roaming users. Regional network prioritization should be set up within the definition of a national QoS framework. The framework defines a set of priority mappings that enable interoperability between LTE regions.

Triggers for Public Safety Broadband Prioritization. Priority for public safety bearers should be automatically determined. Prioritization of associated LTE bearers should be triggered using standard LTE mechanisms (i.e. bearer activation/modification).

Utilization of NGN GETS for Public Safety Broadband Network. There are potential scenarios for public safety that may utilize NGN/GETS capabilities. However, NGN/GETS was developed for use on commercial networks. MSI believes that NGN/GETS is insufficient for public safety usage and should not be used in the broadband public safety network.

10. Mobility and Handover (response to paragraphs 47- 50)

MSI agrees with the Commission's tentative conclusion that each operator's network must support seamless handover within its coverage region. Handover within an operator's network should be supported.

MSI believes that it is not necessary to codify the handover methods. Both X2 and S1 handover have use in certain deployment scenarios. However, some deployments may not

require both types. Further, there may be future handover types which will be better suited for future deployments. As an example, X2-handover will likely be the most common method for intra-vendor links. S1-handover will likely be the most common method used for inter-operator links.

MSI strongly believes that the LTE technology is insufficient to support inter-PLMN handover "day 1" and this should not be mandated. While the LTE standard references inter-PLMN-ID handover, the standard is incomplete in this area and does not sufficiently define how to support this function. Implementing inter-PLMN handover will be gated by implementation of inter-PLMN network planning and network operation organizations. These organizations are needed to ensure coordinated network configurations to enable inter-PLMN handover. Further, these organizations will evolve as driven by the needs of public safety practitioners as their networks become geographically adjacent. In most instances, this will not occur and hence will not be needed on “day 1”. Rather, inter-PLMN handover should be a long-term objective for public safety networks, based on need driven by geographic adjacency.

The Commission also requested comment on the need to establish a minimum speed in miles per hour for handovers. High-speed handover is supported by LTE technology, but it is not necessary for the Commission to set minimum speed criteria in the rules. Implementation of high-speed handover should be optional with the requirements driven based on needs and practicality in a region..

11. Out of Band Emissions and Related Requirements (response to paragraphs 51- 54)

MSI agrees with the Commission’s tentative conclusion regarding an OOBE limit for the nationwide public safety broadband networks.

12. Applications (response to paragraphs 55- 57)

Some of the applications the Commission proposes to require, such as Internet access or agency-controlled VPN access, are already well understood. Others, such as the status or information “homepage”, are not defined beyond high-level descriptions, and will not support interoperability until the necessary specifications are developed. As an example, Field-based Server Applications connectivity using public IP space is well understood, but a framework to enable authentication and authorization to use any applications, for either home or visiting users, still needs to be defined.

Internet Access. Internet access is generally considered to be IP transport to public IP space. Multiple applications run over the internet, from browsers to IM to email. Restricting access to web sites or to use of protocols is a policy decision of each agency. Restrictions can be enforced at the device or by the agency IT network for home routed traffic. Restrictions in visited networks are not recommended. There is no standard way to enforce security policies in the visited network for roamers and is not enforceable for encrypted traffic.

VPN. Two forms of VPN are recommended. A network hosted VPN can provide secure connectivity between the EPC and each agency. The network hosted VPN requires no client software. Use of network hosted VPN should be optional.

Agencies can additionally choose to require a client based VPN. A client based VPN can provide secure communication between the UE device and the agency. This type of solution can be used across public safety LTE, commercial wireless operators, or WiFi service providers. The client based VPN should not require any support from the network for basic operation. QoS support for an encrypted traffic stream containing multiple applications requires integration support not specified in 3GPP standards. However, this aspect will not affect interoperability, as the integration is limited to the agency home network and the device client.

The network should not restrict VPN protocols unless defending against known security risks. Each agency should be able to choose its own VPN protocols and restrictions as appropriate to their IT network and security needs.

Two scenarios may require the use of a network hosted VPN server to support a client based VPN. One scenario is a local break out application that needs to be secured and is not secured at the application level. A framework would need to be developed for authenticating and authorizing users to this service in support of the local breakout application. An alternate approach is to authenticate via the home network and use a network-to-network interface for connectivity to the local application.

The second scenario is the deployment of shared applications across multiple agencies. If the applications cannot provide native security and additional security is required, the regional network could provide VPN servers for the set of hosted applications. This solution is supportable for home users via configuration in the device and the regional network. However, typical client based VPN solutions do not support multiple secure tunnels, and thus do not enable a device to securely connect with its agency and its regional applications simultaneously.

Field based server applications. Device support for field based server applications depends on the application, which has not yet been defined. A web based interface would be simple in terms of required device support. While connectivity is certainly an important issue, the most important issue is authentication and authorization to access and use the application. The application will be visible on the internet and access needs to be secured. MSI continues to suggest an authentication framework based on Security Assertion Markup language (SAML). The network can provide the required connectivity in several different ways but development of such applications requires agreement on an application level authentication framework.

Application restrictions. The only restrictions imposed by the public safety broadband network should be focused on security. Wholesale restrictions on applications, protocols or ports should be left to their local IT policy and enforced on the device itself or in the agency IT network. The broadband network should enforce the subscribers authorized services in terms of bandwidth and QoS while at home and roaming.

NPSTC BBTF Report "desired" applications. Location – Location is an important aspect to the public safety work flow. Typically this is considered a building block application that is utilized via other applications such as Computer Aided Dispatch. The broadband network can support an "over-the-top" location solution using device-based GPS or it can additionally support network-assisted location. Network -assisted solutions are intended to enhance location reporting in scenarios such as in-building. The 3GPP specifications provide standards for both solutions.

The 3GPP solutions for location are designed with commercial carrier based applications in mind (eg, emergency calls and carrier hosted applications). Devices support API's for device based applications to read their location as well. To apply this technology to public safety, some additional specification is required. The agency needs policy controls to determine which applications and which end users are allowed to see a location. Many carrier based solutions are based on user opt-in/out or a single carrier policy and are not tailored for multiple agencies.

One-to-Many – The 3GPP R9 standards include broadcast support using LTE. The main focus was several carrier use cases around multi-media content sharing to the masses. The solution provided so far by standards dedicates precious resource blocks to broadcast and uses OAM&P procedures to add and remove the dedicated channels. Further enhancements are being worked in R10 but it's not clear yet if they will be finished. MSI is hoping that the industry in general develops to the R9 standard but adoption won't be widespread if this is not desired by carriers. Without infrastructure and handset support, developing a public safety solution based on MBMS will likely be too costly.

LMR Voice – The NPSTC Broadband Working Group is developing the requirements for mission critical voice on broadband. Until that effort is complete and a standard approach is adopted for implementing LMR voice on LTE, it is not possible to include this application for inter-operability.

PSTN Voice – There are two major alternatives. The voice solution can be enterprise-oriented and thereby compatible with existing agency PBX's or it can be a commercial carrier-oriented voice solution. An enterprise-oriented solution extends PBX services to wireless devices and provides direct connectivity to landline PBX components. Such a solution can use SIP trunking to efficiently provide connectivity outside of the agency. Commercial carrier voice solutions are optimized for large-scale deployments and voice application-level roaming and for monetization between the home and visited networks. Commercial carrier voice solutions are evolving from circuit based to IMS, both of which require large supporting infrastructures.

Including these additional applications at this time will not contribute to nationwide inter-operability until further application definition occurs. Location and PSTN voice are supported in the R9 version of the standards. One-to-Many and LMR Voice depend on the implementation of of MBMS in both the infrastructure and the device chipsets. General industry adoption of MBMS is not clear at this time because the demand for this feature by commercial carriers is very limited. While the LTE Rel. 9 standards for basic MBMS are complete, product implementation within the industry is still unclear. The industry may wait for enhancements included in the Rel. 10 standards to implement MBMS.

Other applications. For an application to be adopted, the application has to have been standardized. Adoption of the application matters to the broadband public safety system if the application places a new transport requirement on the network that the network is currently not capable of handling. Adoption of the application also matters if the service is intended to be partially or fully served by the visited network in a roaming scenario. It is not clear that any applications beyond the defined set are standardized and ready for adoption.

The public safety industry settled on LTE as its broadband technology due to its capabilities and the scale of the ecosystem. In 3GPP the LTE/EPC architecture provides transport for IP packets. The architecture allows for best effort delivery of those packets and for more demanding applications the architecture supports QoS and admission control. The interface to applications is kept pretty simple and there is a clear separation of the application space from the transport space. Simple applications just use the IP SGi interface. More demanding applications additionally use the Rx interface for QoS and admission control.

To promote the inter-operability of key applications for public safety agencies and users, those applications need to be standardized. 3GPP defines two primary applications using the IMS framework: voice and short message service. Although IMS has been defined for ten years, even most initial LTE deployments rolling out this year still do not utilize the IMS framework. LTE will be a driver to improve the adoption of IMS but only for voice and SMS which will evolve over many more years. The 3GPP commercial carrier market is not interested in standardizing Computer Aided Dispatch or Remote Query or Records management or Evidence Management. That's not a problem because the LTE/EPC network is capable of serving those applications for public safety. Video distribution for public safety and mission critical voice are applications that require additional capabilities still in progress in 3GPP. Once again we should expect 3GPP to provide the transport capabilities and the public safety industry to standardize at the application layer.

Interfaces. Application client to server interfaces and application network-to-network interfaces impact interoperability. IMS standardizes both the client interfaces and the NNI's. This approach was defined to allow monetization of packet traffic and is based on a distributed model where the home operator and the visited operator get to share in the revenue. It's also designed for operator controlled applications running under operator controlled policy. The control for many public safety applications resides at the agency level today, and should remain there in the future. To standardize applications for public safety, a model and a set of applications need to be specified. The transport provided by LTE will be able to support those applications as they are standardized without requiring more than policy updates to the EPC equipment (mainly the PCRF).

Mandating support for additional interfaces would require defining additional elements at the application level. This should be a separate issue from deploying the broadband network. The broadband network may reuse some LMR sites, but is generally going up for the first time with new equipment. The public safety applications are already deployed at most public safety agencies. Getting agreement among the vendors and the agencies on standardizing these currently un-standardized applications will require time.

13. Interconnection With Legacy Public Safety Networks (response to paragraph 58)

Today, public safety agencies have defined private data networks for their legacy state/local data applications. In many cases, public safety agencies also incorporate (M)VPN technologies in these data networks. Existing data applications, such as Computer Aided Dispatch and local video, can benefit from the advantages of throughput, redundancy, and enhanced coverage provided by the PSST LTE spectrum.

By utilizing LTE's standard Access Point Name (APN) technology, an LTE device can support a legacy "agency APN" which enables routing traffic between the device and the agency's legacy data network. LTE devices can utilize these same legacy agency APN's. This will allow an LTE device to integrate with existing public safety data networks and applications. This will further support item #55 (and the NPSTC applications), which requires "VPN access to any authorized site and to home networks" and this strategy also allows an agency to leverage their existing IT infrastructure and applications.

To achieve this, guidelines should be established which allow a local agency to:

(1) create and associate an LTE APN to the agency's existing data networks and promote this APN in national DNS applications and the roaming transport service.

(2) associate LTE QoS policy (PCC rules) with existing agency applications within the confines of the national QoS framework

(3) limit transport costs associated with deploying legacy data applications by enabling regional and tribal networks to deploy localized PGW/SGW elements and associated IP transport equipment

Regarding gateways between existing public safety networks and PSST LTE, physical equipment will be necessary to provide security and interworking between the agency's legacy data network and the LTE system. It will be possible for the gateways to support both voice and data applications. For example, by leveraging a national IP backbone, an existing agency VoIP PBX could interface with a peer agency VoIP PBX in another LTE tribal area, saving the agencies PSTN costs. Many gateways with such capabilities are readily available in industry.

Much of the interoperable capabilities in this question require a nationwide IP backbone. This should be emphasized and established as soon as practical. Once this is in place, data and voice interoperability scenarios will be substantially enabled. A funding and operational plan needs to be created for the deployment and sustainability of this nationwide network.

This nationwide IP backbone can also support an agency's TIA standard TIA-102.BACA-A (a.k.a. ISSI) interface to another agency on the backbone. This will help facilitate the interconnection of P25 systems.

14. Performance (response to paragraphs 59- 62)

MSI also recognizes the importance of ensuring efficient use of spectrum in public safety broadband networks. Performance requirements can help ensure baseline operability, but they should be carefully defined to correspond to the unique geographic morphologies and usage/loading profiles that will be found both between and within broadband networks.

The substantial improvements on mobile data network performance in recent years have been achieved by full exploitation of spectrum resources and dynamic sharing of cell resources (e.g. via single frequency reuse). These same factors, however, also cause a wide variation in the user data rate depending upon the user location within the cell area and the network loading.

There is also an inherent trade-off between cell edge UE throughput and sector throughput which is determined based on the eNB scheduler implementation

Cell edge throughput is primarily a function of eNB and UE specifications as well as cell edge SINR, with the latter influenced by such factors as inter-site distance (ISD), eNB antenna heights, RF environment, and interference due to neighbor-cells. As public safety entities have various geographical and economic constraints, they require radio design and deployment flexibility for their broadband networks. For these reasons, MSI feels that if minimum cell edge data rates are defined, then these requirements must also allow flexibility associated with the various morphologies (i.e., cell site densities), user densities, loading assumptions, and application traffic profiles that will exist within and between the networks. This approach ensures a minimum level of performance and interoperability while allowing for realistic and practical system design and usage.

Any RF performance requirements defined with fixed data rates must allow for variance on these factors. Specifying requirements associated with these factors may preclude network deployment for many public safety entities, which could actually undermine the Commission's interoperability goal. In addition, if data rate is defined as physical layer rate then the demarcation point at which the minimum data rates are measured should be well-defined. In this case, then perhaps the demarcation point can be defined by referencing a standards document such as 3GPP TS 36.321 (Figure 4.2.1.1). However, MSI recommends that the data rate should be defined closer to the application layer, such as the UDP payload data rates. The reasons are that data rates specified at this layer are representative of rates that users would experience in system operation, and the data rates can be easily measured with off-the-shelf tools and monitors. We believe that application-layer data rate specification is also consistent with the NPSTC SoR requirements.

Regarding the proposed requirement for "each public safety network operator to certify, within thirty days of its date of service availability, that its network is capable of achieving these data rates", MSI feels that the time frame for compliance should be much greater than thirty days to allow for system optimization and drive testing. The required time frame will also depend on the size of the geographic area being tested. To account for such issues, a 12 month timeframe after service availability for compliance would be more reasonable. The appropriate geographic areas for making data rate certification measurements should be defined by each public safety entity, taking into account factors such as roll-out issues, cost, and time.

MSI does not feel that any additional performance requirements are needed to enable interoperable public safety broadband networks nationwide. Where performance requirements are defined, they should be specified in terms of data rate or perhaps received signal levels, rather than spectral efficiency. Spectral efficiency can be improved through various interference mitigation schemes, but when such schemes achieve these gains by limiting radio resource block allocation, the net data rates are very often lower than without interference mitigation. As user experience is based on delivered data rates, the data rates are MSI's preferred performance metrics.

Performance certification should be limited to covered area reliability for a specified UDP throughput. Covered area reliability, as defined in TSB-88, is widely accepted by the

public safety community as the metric with which network performance is characterized. Only simulated coverage certification plots should be required as it will be very difficult to define consistent and controlled drive test conditions, especially UL interference (neighbor-cell) loading. Also, coverage maps should not be required at each phase, nor should additional updates be required beyond the initial coverage validation. Both of these requirements would place significant extra cost and burden on the public safety operator. The essential validations should be limited to the system design, rather than on-going system performance.

As discussed in the comments above, MSI feels that a fixed sector loading assumption should not be defined in conjunction with the minimum data rate requirements. Instead, loading should be a system design variable per network, based on each public safety entity's traffic model, determined based on application data rates, usage model, user profiles, user density, and morphology.

15. Network Capacity (response to paragraphs 63- 64)

MSI agrees that first generation public safety broadband networks should be upgradeable to capture efficiency gains available via advanced features supported by future versions of the LTE standard.

Any network backhaul system normally incorporates a hierarchal layer of multiple backhaul connections in various parts of the overall network. Not all backhaul hierarchal levels in the network will have the same capacity requirements. While a lower hierarchal level backhaul link would need to support the maximum potential traffic for a connected cell, higher level backhaul links generally would not need a capacity equivalent to the aggregate maximum capacity of every cell in the network because not all cells are likely to be at maximum capacity at the same time. In a public safety system, aggregated backhaul resources at the higher hierarchal levels should optimally be sized for normal "busy hour" capacity, and not for incident capacity. The difference between average loading and busy hour could be 2x or 3x. A jump in incident capacity could be greater than 10x on a given cell. That is, a lot of extra capacity to carry in every backhaul link throughout the system. A larger system with a large subscriber base could easily fully load a cell under incident. Although additional responders can be brought in from adjacent systems, there is no expectation that all cells can be loaded at the same time. A more remote system built for coverage may be more than adequate if the backhaul and not the cell capacity is the blocking factor. It should be the regional networks choice how much edge of the network backhaul capacity they maintain based on their ability to fund and maintain that capacity. It should also be their choice how much aggregation they plan for. If traffic is properly prioritized, the important traffic will be delivered through congested links.

Simply setting a minimum level for backhaul and core over-simplifies the problem and results in an inefficient solution. Backhaul capacity should be set for the peak capacity that an eNB might see during an incident tempered by what resources are available to the regional network operator. Backhaul aggregation can be utilized so that incident capacity for every eNB is only needed on the last segment of the backhaul to the eNB. The minimum level needs to support the average busy hour demand under the expected user load and call model. Core capacity, on the other hand, is less affected by incident bandwidth. Core capacity should be determined by the expected number of active UEs (home users, roamers/mutual aid) and their

call model. The core capacity usage should be monitored over time to determine changes in the call model or changes in the percentage of active users.

One could envisage a scenario where all sectors within a site need to go to incident capacity simultaneously. However, if the most likely incident scenario only fully loads a portion of the sectors at any given eNB, then paying for additional bandwidth may require unsustainable costs associated with equipment and on-going operations. The network operator should be given some latitude in designing the backhaul network. If 20 Mbps is significantly cheaper due to loading on a microwave ring, then that level may be sufficient. If dark fiber is available to each eNB, then extra bandwidth may come at little or no extra cost.

An operator should account for some level of incident support at each eNB plus some level of aggregation in the backhaul network. It is unlikely that every site in the system will be under incident simultaneously. The backhaul capacity into the core should not be the number of eNB's multiplied by the incident bandwidth required on the last mile to an eNB.

The capacity of the core should be sized based on the number of subscribers expected and the call model. The number of subscribers should account for roamers and mutual aid devices. It is likely that most of the responders to an incident will come from the first responders belonging to that system and, although they will cause extra capacity at a site, they will not present extra load on the core. Under certain scenarios, backhaul at the site could be the limiting capacity factor, but capacity limitations will not impact interoperability. Proper use of QoS and priority should insure that the most important traffic gets the required bandwidth. Requiring the maximum amount of backhaul capacity to each eNB will require additional equipment and microwave license costs if the backhaul is purchased, or additional monthly costs if the backhaul is leased.

16. Security and Encryption (response to paragraphs 65- 69)

MSI agrees that Network Access Security (I) and Network Domain Security (II) are essential for broadband public safety security. TS 33.401 and TS 33.210 are sufficient to ensure the security of the LTE air interface.

User domain security (III) which is described in 33.102 involves users authenticating to the Universal Subscriber Identity Module (USIM) card within a UE itself. For handheld devices with an integrated USIM, this would typically involve prompting the user to enter a PIN to unlock the USIM prior to accessing specific applications on the USIM (such as a phone book, or SMS storage). From MSI's perspective this applies in a limited way to public safety. First, not all classes of devices will utilize the USIM to store information requiring this type of access control. A USB modem or embedded vehicular form factors are unlikely to require interaction with the USIM to store user sensitive information. Second, it should be the policy of the agency and/or individual using the device to determine the user's security requirements for access to sensitive information on the USIM card itself. Third, from the perspective of the CJIS security policy requirements for access to national databases like NCIC, USIM PIN based unlocking of the device is insufficient.

Application domain security (IV) in the context of 3GPP LTE specifications is a reference to TS 31.111 which describes the USIM Application toolkit with TS 23.048 defining security mechanisms that provide access to the USIM. The purpose of these specifications is to provide operators with secure access mechanisms to the USIM itself to manage key information objects on the USIM such as the list of preferred roaming partner PLMNs and other information. MSI agrees that support for the USIM Application toolkit should be incorporated into public safety LTE devices. In practice USIM management applications are coordinated with the USIMs used by the operator.

With regard to Visibility and Configurability of Security (V), MSI recommends that the FCC not mandate specific rules. The Visibility and Configurability of Security specifications are targeted to handheld devices with a User Interface accessible to the end user. 3GPP does not take into account the prevalent use of VPN or Mobile VPN products used by public safety. It is these products that provide the end to end security that many public safety agencies typically are most interested in. For these applications having user visible and/or configurable security controls for the LTE interface will likely confuse the typical end user of a public safety device. The vendors of the VPN products utilized (including those of public safety computing devices utilizing USB modems or in-vehicle devices) will be responsible for providing the appropriate user visibility and configurability to the security capabilities of the software. Finally, for public safety we expect that agencies would not expect or require their users to do any security related configuration of the device. We expect that the public safety agencies will take it upon themselves to administer agency security policies in a centralized fashion.

The optional security features specified in TS 33.401 may be referenced for public safety broadband networks. These security features provide integrity protection and encryption for the control and user bearer traffic for three interfaces within the system namely: UE- eNB Radio Resource Control, UE-MME control messages, and UE-eNB user data traffic. MSI recommends the default use of 128-EEA2 (128-bit AES) to cipher the RRC, NAS and user plane messages and 128-EIA2 (128-bit AES) for NAS and RRC message integrity-protection as opposed to the 3GPP SNOW3G algorithms. The recommendation is due to the NIST Federal Information Processing Standard (FIPS) approval of 128-bit AES as an approved cryptographic algorithm. SNOW3G has not been evaluated by the NIST FIPS.

With regard to the sufficiency of TS 33.401 for the public safety environment, MSI considers this specification sufficient. It is also worth noting that many public safety agencies require the use of FIPS-140-2 certified VPN or Mobile VPN security products to provide end to end security. These products will likely be deployed in many public safety LTE environments. When combined with the security capabilities of the TS 33.401 public safety's security needs are adequately met.

The TS 33.210 specification defines mechanisms to secure communications within a given network domain as well as the communication that occurs between network domains. It is MSI's view that public safety LTE networks should be responsible for the security of the communication within the network domain that they administer according to their own security policies. Communication between eNBs and the EPC of a particular public safety broadband system may be protected using IPSec. 3GPP considers this an intra-domain security interface (aka, Zb interface) and states that securing this is optional. In MSI's view we do not think it wise

to require intra-domain security. It is possible that alternative technologies can be used to secure the intra-domain links. For example, link security can be provided by dedicated microwave backhaul technologies. In other cases, the backhaul networks may be part of a Metro Area Ethernet network shared with other users and therefore warrants the need to include IPSec for the S1 interfaces. Depending on how the public safety broadband equipment is deployed physically it may or may not benefit from having IPSec for interfaces such as S5, S6a, S8, S11 and Gx. Equipment may well be co-located in the same facility and thereby be under significantly less risk for malicious attack. Clearly within the facility good IP planning including the use prodigious use of network segmentation and access controls will improve the overall system robustness, however the Commission should attempt to define the rules around these network links.

For the interfaces between public safety broadband network facilities the security expectations for these interfaces depends on how the broadband networks are interconnected. If, for example, a roaming service provider is used to enable inter-network communication, each individual public safety network need only establish a secured connection to that network and allow that roaming service provider to establish the trusted links to the peer networks in a hub and spoke like architecture. MSI recommends that GSMA IR.77 "Inter-Operator IP Backbone Security Requirements for Service Providers and Inter-operator IP backbone Providers" be applied to the IP Backbone that is providing the roaming service provider function for public safety.

If on the other hand, public safety networks establish their own peering interfaces in a fully meshed fashion, then it will be necessary for each agency to manage their own security associations with each peer.

As mentioned in response to the Application security point in question #65. Application domain security in the context of 3GPP is related to USIM application Toolkit. MSI does not foresee the need for the FCC to specify rules concerning the applications present on the USIM since there is a direct relationship between the home network and the USIMs used with the home network. Therefore rules concerning interoperability are not required.

The 3GPP TS 33.102 specifications were written assuming hand held consumer class devices as their baseline. The specifications place much of the responsibility for secure communication verification into the hands of the end user. In MSI's opinion this approach is not well suited to the public safety environment. It is MSI's expectation that public safety agencies will leverage VPN or Mobile VPN technologies that will provide their own security 'visibility' and 'configurability' capabilities to the public safety environment. For these reasons, the Commission should not adopt rules for visibility and configurability of security.

17. Robustness and Hardening (response to paragraph 70)

With respect to emergency power, the Commission should recommend emergency power and then allow public safety entities to decide how much is needed based on their particular needs and circumstances. The public safety entity should also be able to determine how they want to deliver emergency power solutions. In some cases, the LTE equipment will be collocated with existing voice radio networks and the public safety entity may want to use or

expand the existing emergency power source so that there are not multiple power systems in the shelter. Other times public safety entity will require solar or some other available power source.

Backup time recommendations should be a function of the site accessibility; for example, sites located in remote areas should have higher backup time than sites located in areas easily accessible for a repair. Similarly sites in critical locations e.g. downtown or crowded areas should have higher backup time because of the scale of a down time effect.

18. Coverage Requirements (response to paragraphs 71- 73)

MSI's view is that the FCC should not impose coverage and performance requirements. The FCC should not require population or geographic benchmarks for coverage and performance. MSI believes it would be very difficult to create a set of coverage and performance requirements that would work well for all public safety organizations. MSI supports the view that each public safety entity should be allowed to make coverage and performance decisions based on how to best serve their community. If, however, the FCC decides to impose coverage and performance requirements, MSI encourages the Commission to consider a self certification validation process.

The FCC should not require vehicle count or other benchmarks in order to promote coverage of major highways and interstates through rural areas. If the FCC wishes to impose such requirements, said requirements should be tied to specific funding of rural coverage.

19. Coverage Reliability (response to paragraphs 74- 75)

MSI favors having each public safety network supplier provide to the public safety entity an initial assessment of coverage and performance for each round of PUBLIC SAFETY funding. Access to high quality coverage and performance information will enable each public safety entity to make their own coverage and performance decisions based on how to best serve their community.

MSI agrees that the network should provide outdoor coverage reliability at a probability of coverage of 95 percent for all services and applications throughout the network. MSI does not agree with including a coverage reliability requirement for indoor environments. MSI believes it would be very difficult to create a set of coverage and performance requirements that would work well for all indoor environments. RF penetration into an indoor environment is dependent upon many factors including: the frequency of the communication network, the height of the tower, the height and depth of the building, the location of the building relative to the base site, the amount of log normal shadowing due to nearby buildings, the building materials, and the maximum number of walls that must be penetrated. Buildings with metal walls for offices and the metal enclosures around elevator shafts are particularly difficult to cover. Each public safety entity should be allowed to make indoor coverage and performance decisions based on how to best serve their community.

20. Interference Coordination (response to paragraphs 76- 79)

MSI agrees with the importance of coordinated planning for deployment of geographically adjacent or bordering networks to mitigate interference issues. Although the LTE

physical layer is designed to tolerate and operate effectively in the presence of interference, avoiding difficult interference scenarios between networks is a logical step whenever possible.

MSI agrees that notification of deployment plans should be required. However, we feel that notification 90 days before deployment does not provide enough time for negotiation and planning. Once initial waiver systems are deployed, we believe that nine to twelve months would be more appropriate for notification of additional regional deployments .

The LTE physical layer was designed from its inception to operate effectively with the high interference and low cell-edge SINR levels that are characteristic of single-frequency reuse systems. Robust control channel and reference signal designs as well as HARQ for the data channels are among the design features that make this possible. In certain cases, and typically only at lower loading levels, cell edge throughput can be improved through the use of interference coordination schemes.

Static inter cell interference coordination (ICIC) solutions improve cell-edge SINR by restricting radio resource availability for the entire cell and/or the cell-edge users. So spectral efficiency is typically improved, especially at the cell-edge, but with fewer radio resources available, net cell-edge data rates often do not improve. In other words, whether the spectral efficiency increase offsets the "cost" of reduced usable bandwidth is a function of many variables including loading and network topology. Static ICIC imposes an artificial reduction in average sector capacity as well. Another cost inherent to static ICIC is the need for time-consuming manual coordination and maintenance updates within and between networks. This can be especially disruptive to networks that are already in service.

Semi-static ICIC solutions utilize inter-cell communication (via X2 interface) of loading and interference statistics to reduce interference. In theory, such solutions can provide good system performance gains, but practical solutions are immature and must overcome such issues as delay and loading on the X2 interface as well as stability vs. convergence time tradeoffs. And as with other ICIC solutions, semi-static ICIC only provides performance gains in lower loading cases.

Alternative interference coordination and mitigation schemes are possible. Typically, these schemes involve autonomous interference mitigation techniques within each eNB, independent of neighboring eNB's. These approaches can also provide significant cell edge data rate gains under lower system loading while avoiding the complexity and implementation issues of the schemes outlined above.

MSI feels that specific interference mitigation techniques should not be regulated. Instead, interference within and between regions should first be considered and minimized in the planning phase. Beyond that, whether and what type of interference mitigation solution is utilized should be considered an aspect of the network design and maintenance. Since interference mitigation is a key element of system performance, vendors will continuously innovate and develop a wide range of solutions which can be applied on a case-by-case basis.

MSI supports the Commission's proposal to require public safety broadband networks to coordinate with operators in adjacent spectrum and to take necessary steps to ensure that the

performance of the public safety network is not degraded below the required levels due to interference from spectrally adjacent networks.

B. Public Safety Roaming on Public Safety Broadband Networks

As discussed in more detail in MSI's comments, MSI agrees with the Commission that public safety users must have the ability to roam on all other 700 MHz public safety broadband networks. MSI supplements it comments regarding public safety roaming with the following responses to the questions asked in the *Fourth Notice.*

Nomenclature. The Commission proposes defining a 700 MHz public safety roamer as "A public safety user receiving service from a PLMN other than one to which they are a subscriber." MSI recommends adding a qualifier to this definition to distinguish roaming on commercial carrier network from roaming on another public safety network. The NPSTC Broadband Task Force Report defined roaming between public safety networks as intra-system roaming, and roaming between public safety and commercial carrier networks as inter-system roaming. Since there is precedent for these definitions, MSI recommend adopting them as defined therein. It is not necessary to qualify the mission in the general roaming sense, but mission classification may be useful to support a nationwide roaming QoS framework.

1. Prioritization and Quality of Service to Support Roaming (response to paragraphs 90- 92)

Each region should have the ability to specify the prioritization in their specific region based on their regional criteria. In the context of a national priority framework, the specification needs to include interoperability across regions for prioritization. The framework should require adherence to LTE QCI/ARP standards. It also is required to enable the regional operator to specify prioritization attributes within a region while accommodating prioritization for visiting users in the region. Interoperability is assured by enabling a mapping of priorities into classes ("buckets"), and consistent implementation of the priority "buckets" in each of the regions. Roamers within the LTE private public safety network would be mapped to priority "buckets" in accordance with the inter-regional mapping scheme.

Priority for public safety should be automatically determined and invoked within the system. Determination of priority should not distract responders or dispatchers from the mission at hand. Prioritization should be triggered using standard LTE mechanisms (ie, bearer activation/modification). Prioritization triggers can take many forms.. However, the framework (i.e. QCI, ARP) from which the prioritization is assigned should be agreed upon by the regional operators/agencies, and would be utilized to determine the resultant priority based on the specific triggering event.

The regional/local entity that is operating the public safety LTE network should have authority to dictate prioritization within the scope of their jurisdiction. There must be agreement between relevant entities as to the specific prioritization values, and must be provisioned as such into the LTE system prioritization policies. The entire LTE system needs to have a well-defined, extensible framework that works for roamers that allows local assignment of priority within each "bucket". The actual priority assigned to a regional or local agency would be provisioned within

the public safety LTE network policies, and said policies would be deployed upon receipt of a specific prioritization trigger.

There are potential scenarios for public safety that may utilize NGN/GETS capabilities. However, NGN/GETS was developed for use on commercial networks. It is important to note that NGN/GETS is not designed for use by public safety and should not be relied upon for triggering of public safety network access. In NGN/GETS, the end-user triggers the system to set up appropriate priority in the network, however for public safety work flows, such triggering is likely to originate elsewhere, (*i.e.*, dispatch operators).

Regional network prioritization should be set up within the definition of a national QoS framework. This prioritization framework will likely be needed across all regional LTE systems. The framework defines a set of priority mappings that enable interoperability between LTE regions. This framework also allows for regional operators to specify their specific priority based on regional needs.

2. Applications to Be Supported (response to paragraph 93)

Internet access. Internet access can be provided to roamers via home routing or local breakout. Home routing allows local IT policy to be implemented by the home IT network. Local breakout provides potentially lower cost internet access while roaming, although this is not expected to be significant due to low volumes associated with internet traffic while roaming. Using local breakout puts an additional burden on the visited network to provide public IP addresses to the devices or provide a Network Address Translation (NAT) service to the internet. The NAT service has the capability of breaking some legacy applications.

VPN access to any authorized site and to home networks. Agency provided VPN access to the home network can be accomplished with mobile VPN software (clients on the device and servers in the home network) available today.

The EPC can also support a hosted VPN service where traffic for all devices belonging to an agency is tunneled to the agency. This service is only available from the home PGW, thus requiring home routed service while roaming.

A status or information "homepage." The 3GPP standards provide sufficient tools to enable connectivity to a status or information home page. However, the application and the access control to such an application are not sufficiently defined to assure inter-operability while roaming. Web standards are sufficient to assure display of such a page on a device. Additional specification is required to limit access to the information on a page by page basis to the correct set of responders. Additional specification is required to support functions such as client updates via over-the-air downloads (assuming a multi-vendor and multi-OS device environment).

Field based server applications. The 3GPP standards provide sufficient tools to support connectivity to a field based server application. Assuming that the server application is hosted in public IP space (per footnote 70 in paragraph 55), a device can obtain transport access via local breakout to the internet or home routed access via their agency internet access. However, the application specification and the access control to such an application are not sufficiently defined to assure inter-operability while roaming.

Additional application. Applications common to public safety include computer aided dispatch, remote records query, report generation, evidence management in addition to LMR mission critical voice. Home routed roaming service allows these data applications to be accesses while roaming. Using local breakout would require that these applications and their associated client interfaces be standardized and/or associated network-to-network interfaces be standardized. This standardization would be independent (ie, out of scope) of the 3GPP LTE/EPC standards.

Work has begun on mission critical voice requirements in the NPSTC Broadband Working Group. However, the specification is not far enough along to be implemented.

3. Public Safety-to-Public Safety Roaming Rates (response to paragraphs 94-97)

Roaming service charges should not be regulated by the Commission. Roaming service fees should not be based on monthly service data charges for wireless voice and data services. Rather, roaming fees should be based on actual service usage and actual operating costs. Roaming service reciprocity will likely be extended to adjacent regional networks to facilitate mutual aid, and thus will minimize the need for roaming service fees among public safety entities. Intra-system roaming will be implemented to protect the safety of citizens, and not to generate surplus revenue. Unlike commercial carriers, we anticipate that revenue generation will not be a significant driver for implementing intra-system roaming.

4. Proposed Model Agreement (response to paragraphs 98-99)

It is not necessary for the FCC to establish a standard roaming agreement. Public safety entities should be afforded the latitude to select and modify roaming agreements based on their needs and benefit from open competition in the market.

The Commission requests comments on the need for a standard roaming agreement for public safety intra-system roaming. MSI believes this is primarily an issue for public safety entities to address. Because the available capacity and prioritization to support roaming could vary across jurisdictions and within the same jurisdiction at different incidents, we expect there would need to be some local/regional tailoring of roaming agreements, which may also evolve over time.

C. Federal Use

1. Section 2.103 (response to paragraphs 100-103)

In its Order issued May 12, 2010 which granted conditional waivers to 21 public safety petitioners to move forward with broadband deployment in their respective areas, the Commission reaffirmed that Federal users are eligible as users on the systems. In the Fourth FNPRM, the Commission seeks additional comment regarding how Federal use should be governed, i.e., at the regional and/or national level. MSI supports Federal users as eligible users on the broadband network. Allowin federal users to be on the same band with local and state entities from the outset of broadband deployment will provide a firm foundation for interoperability across multiple levels of government.

The issues raised by the Commission regarding governance are largely issues for which agencies deploying broadband systems in their respective regions in consultation with the PSBL should decide. In any geographic area there needs to be local control of the network, married with any nationwide control needed to ensure interoperability. Local control includes the ability to properly prioritize use of the network to meet the communications needs at all locations in the region, and that prioritization would apply to all users, including Federal users.

Prioritization among users on the system should not be static, and will likely need to be adjusted to match the location and timing of various prevention and response activities. In addition, specific Federal needs may vary, e.g., the needs in the Washington, DC area may be quite different than those in Seattle or along the Mexican border, etc. Accordingly, MSI believes that any governance agreements regarding Federal use of the network may involve multiple authorities with a stake in local public safety broadband deployment. It may be possible to develop a Federal user agreement guideline which would then be customized as needed by region. MSI sees this as a governance task, in consultation and coordination with the regions and potential Federal users, not as a Commission rule.

2. Roaming (response to paragraphs 104-105)

The Commission also seeks comment on the appropriate regime for allowing Federal users to roam onto state or local public safety broadband systems. MSI believes that priority level assignment for visiting Federal users should be governed as part of roaming agreements and determined, in part, by technical and operational capabilities of the participating networks.

Under spectrum leasing, we believe that Federal agencies would be eligible to use intra-system roaming. We note, however, that LTE technology dictates that spectrum leases must cover distinctly separate geographic coverage areas.

D. Testing and Verification to Ensure Interoperability

1. Conformance Testing (response to paragraphs 106-108)

The Commission also seeks comment on whether all user devices should be subject to conformance testing. We agree that all user devices should be subject to conformance testing to ensure basic device-network interoperability. Just as with devices on commercial networks, there can be differentiation across different public safety devices while interoperability is maintained.

MSI agrees with the Commission that a six month timeline is sufficient to complete testing for initial devices. Any new / modified rules should apply to devices which are deployed six months after the ruling goes into effect. That is, device manufacturers should be given at least 6 months to lock down the conformance requirements for devices under development.

Early Inter-Operability Testing (IOT) for LTE infrastructure was facilitated by industry consortiums, such as the Network Vendors IOT (NVIOT) forum and the LTE/SAE Trial Initiative (LSTi).[5]

At the current maturity level of LTE technology, conformance testing for LTE infrastructure is typically conducted by commercial network operators. Public safety operators should consider IOT involvement as part of vendor selection and evaluation. However, specific IOT requirements should not be regulated.

2. Interoperability Testing (IOT) (response to paragraphs 109 - 115)

Multi-vendor interoperability is an economic consideration which is most appropriately determined by public safety operators. The Commission's rules should be oriented toward interoperability among public safety networks, and not among vendor equipment. As such, the IOT interfaces should be limited to roaming interfaces which extend across operator networks. These interfaces are:

- S6a – between MME and HSS
- S8 – between SGW and PGW
- S9 – between Home PCRF and Visited PCRF

For roaming, the S6a interface is required to support both home routed and local breakout roaming. The S8 interface usage is limited to supporting home routed roaming. The S9 interface usage is limited to supporting local breakout roaming.

The GSM Association (GSMA) provides permanent reference document (PRD) specifications to facilitate roaming interconnection of 3GPP networks. As examples, GSMA PRD IR.88 provides LTE Roaming Guidelines, and further references PRD specifications IR.33, IR.34, IR.40, and IR.67. These documents outline an interconnection architecture involving an IP eXchange (IPX) network. In lieu of a national public safety roaming backbone, implementing the S8 interface between public safety networks will require support of an IPX-based commercial roaming service provider. However, early PUBLIC SAFETY LTE adopters will have limited roaming partner opportunities due to a small number of disparate networks deployed across the country. Further, S8 implementation requires a service contract and associated interconnect fees paid to the roaming service provider. Roaming service provider interconnect fees can be significant. Since roaming usage will be practically limited until significant numbers of PUBLIC SAFETY networks are available, the compliance criteria to support this interface should be based on an aggregate number of in-service networks rather than service availability of any one network. Further, we note that it is feasible to implement the S8 interface via an upgrade to the EPC, and doing so does not require decommissioning or replacing deployed equipment. For these reasons, we respectfully suggest that service availability of at least four networks should be attained before the requirement to support the S8 interface shall become effective.

[5] For additional information on the status and output of these organizations, please reference www.nviot-forum.org and http://www.lstiforum.org/file/news/LSTI_presentation_London_Oct_2010.pdf.

Similar to the S8 interface, implementation of the S9 interface requires interconnecting via a roaming service provider. The S9 implementation compliance criteria should be based on a minimum number of networks attaining service availability. We respectfully suggest that an S9 interface implementation period of at least 18 months after a minimum of four networks have attained service availability.

We believe that it is overly burdensome for public safety operators and vendors to conduct IOT on an ongoing basis for all LTE capabilities, and to be sufficiently broad to include all functions required under the waiver order. Rather, it is reasonable and sufficient to require public safety network operators to achieve interoperable operation upon terms of their mutual agreement. The waiver networks will be operating on an interim basis, and it is likely that the network capabilities will be evolving during that period. Thus, it is premature to require such stringent IOT schedules and ongoing certification by the Bureau.

Vendor labs are already available and capable of conducting IOT for public safety broadband networks; therefore, designation of a public safety IOT lab is not required. Because vendors operate such labs, additional operational costs for IOT would not be required. In this case, vendors and public safety operators would create the test plans and manage the IOT activities.

Third party labs are commercially available to certify compliance to 3GPP specifications for the Uu interface. In this case, the third party labs develop and manage the compliance tests based on 3GPP specifications. Given the eventuality of a multitude of public safety LTE devices, third party certification labs will likely be needed to complete certification compliance in a timely fashion.

3. Interoperability Verification (response to paragraph 116)

Conformance testing is appropriate for the Uu interface. IOT is appropriate for the S6a, S8, and S9 interfaces. IOT does not require independent certification, but rather only self-certified statements of completion. Other interfaces are typically not exposed across networks, and thus do not require IOT or compliance certification.

E. Other Matters Relevant to Interoperability on Public Safety Broadband Networks

1. Network Operations, Administration and Maintenance (response to paragraph 117)

The Commission asks whether operational capacity should be required in order to ensure interoperability of the network. Most entities deploying public safety LTE will have existing narrowband or enterprise systems they already plan, install, operate and optimize. These entities have existing processes and workflows for narrowband and enterprise operations. The operating costs associated with adding public safety LTE operations will be minimized if public safety LTE fits into the existing operations models and workflows utilized by these entities. A mandated operational model or set of practices for LTE will likely result in higher operating costs for the regional/tribal operators and agency IT departments because they will now have to support the mandated LTE operations model/processes as well as their existing operations

model/processes. Consequently, standardized operational models will be counter-productive and increase operating costs, and are therefore not recommended.

Network operations exhibit the following points of interoperability that should be considered:

- Billing information for roamers will need to be shared with either a billing clearinghouse and/or the roamer's home network billing system. It would be advantageous to standardize the charging record format and billing processes for Public safety roaming (e.g. TAP3 records and processes).
- Radio Access Network configurations for border cells between systems must be coordinated. It is recommended that automatic configuration mechanisms, such as 3GPPs Self-Organizing Network (SON) Automatic Neighbor List (ANR) and Physical Cell ID (PCI) assignment, should be disabled in border cells and instead utilize manual assignments as agreed upon by the adjacent operators.

2. Reporting on Network Deployment (response to paragraph 118)

Network planning and deployment must be carefully managed activities, utilizing significant project oversight and formal project management processes and procedures by the network operator. A network rollout plan must be proposed, reviewed, typically contracted with third party installers and tradespersons, and carefully monitored by the network operator. Additional layers of oversight or reporting in this planning and deployment of the network will likely not provide additional benefit beyond what was already provided by common industry practices.

The network deployment phase needs to remain flexible in order to meet schedules and minimize costs. It's not unusual to change deployment strategy for a particular week in order to keep third party installers highly utilized. If, for example, the backhaul provider will not be able to deliver backhaul to a particular geographic area by an agreed upon date, the cell site installers will typically be re-assigned to an area where backhaul is available and installation/validation/commissioning of sites can be completed in a single visit. Requiring an additional level of reporting will make the planning and deployment process less flexible, will slow network planning and deployment activities, and will be a distraction to the project managers that need to carefully monitor the network planning and deployment tasks and milestones.

3. Devices (response to paragraphs 119 - 122)

Channel Bandwidths. We agree that 5+5 and 10+10 MHz bandwidths should be required. Devices should not be required to support 1.3 or 3 MHz channel bandwidths. Disadvantages of 1.3/3 MHz include: inefficiencies due to high channel overhead, increased complexity and cost for devices, and increased complexity and cost for interoperability testing.

Band Class 14 Support. We propose that 5+5 and 10+10 MHz bandwidths should be required for all public safety devices. Supporting 10+10 MHz bandwidth increases device applicability and flexibility as D block allocation is resolved.

Multiple mode support. For interoperability only LTE should be required. In addition to LTE, devices may choose to implement a 2G/3G or satellite capability, but it should not be required.

4. In-Building Communications (response to paragraphs 123 - 126)

MSI agrees that design of a network to provide indoor coverage is extremely challenging. MSI does not support designing networks with additional RF margins in order to provide indoor coverage. This approach could increase both cost and interference in certain scenarios.

MSI believes it would be very difficult to create rules for RF margins that would work well for all environments (eg, urban, suburban, rural) and building types. MSI's opinion is that each public safety entity should be allowed to make indoor coverage decisions based on how to best serve their community.

MSI does not support requirements stipulating that networks be designed with additional RF margins in order to provide indoor coverage. Such an absolute requirement for indoor coverage could significantly raise the cost of systems. Public safety agencies deploying systems will need to have flexibility in defining coverage requirements to meet their needs and to conform to the amount and timing of funding availability. Absolute requirements for in-building coverage at the outset could be counterproductive. If such coverage could not be met economically, then the requirements could actually discourage certain deployments.

Also, system designers need to have flexibility in the best ways to meet the requirements that public safety agencies establish for the build-out in their respective areas at a given time. MSI supports the use of indoor coverage equipment such as Distributed Antenna System (DAS) and picocells as a cost effective means of providing coverage extensions into buildings for future upgrades of public safety broadband systems.

MSI supports the use of Distributed Antenna Systems (DAS) and/or picocells as a means of providing cost effective indoor coverage. Broadband DAS solutions exist that can allow public safety to share some of the cost of indoor coverage with commercial cellular providers.

5. Deployable Assets (response to paragraphs 127 - 128)

MSI supports the use of deployable equipment such as Cell On Wheels (COWS) and Cell On Light Trucks (COLTS) to supplement existing coverage and capacity and to provide a source of network redundancy. MSI does not support requiring the use of 4.9GHz or Satellite bands for backhaul of COWS and COLTS. Public safety entities have different local spectral environments and have different costs associated with use of different types of backhaul based on local circumstances. MSI's opinion is that each public safety entity should be allowed to make backhaul decisions based on how to best serve their community with their available resources.

6. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum (response to paragraphs 129 – 131)

MSI agrees that fixed (point to point) use of 700MHz public safety broadband spectrum should only be allowed on an ancillary basis. MSI believes that mixed use of fixed and mobile services could introduce unacceptable interference.

The FCC has several options that could impact the 4.9GHz and 700MHz broadband networks. These include:

- Mandate the use of 4.9GHz for mobile broadband.
- Mandate the use of 4.9GHz for public safety backhaul instead of 6-38GHz
- Create a "use it or lose it" policy for 4.9GHz band. If they don't use it turn it over to unlicensed.
- Subsidize deployment through special grants.

One issue facing use of the 4.9GHz band spectrum is additional equipment cost. Some of the above options may provide economies of scale which may result in higher volumes and a reduction in equipment cost. Further study would be needed to determine which options are optimum for specific usage scenarios.

Another issue with use of the 4.9GHz band is inter-band interference. MSI would support mechanisms coordinating use of the 4.9GHz band, as the lack of good coordination is causing interference issues between current users.

The 4.9 GHz band could be used to supplement the 700 MHz public safety mobile broadband spectrum particularly for offloading video. Current 802.11n technology will be widely available in the 4.9GHz band and can provide backend interoperability as both these data technologies run on IP networks.

With the advent of public safety broadband there is going to be a need for broadband backhaul links. Some public safety entities will decide to use 4.9GHz and some will opt for licensed microwave for backhaul. Regulatory changes that dedicate a fixed portion of the band to point-to-point use and provide a reasonable coordination mechanism would help enable the use of 4.9GHz spectrum for PUBLIC SAFETY broadband backhaul.

7. Public Safety Broadband and Next-Generation 911 Networks (response to paragraph 133)

The NG911 system will depend upon the availability of robust broadband resources, from the perspectives of both the commercial network operators for citizen use and the public safety community for emergency response. Emergency call related information can be content from citizens or non-human sources such as emergency crash notification systems and sensors. Additionally, NG911 systems can make information available related to the persons involved in the incident (such as medical information) or related the location of the incident (such as building blueprints or video cameras inside the building). It is important that this information does not stop at the communications center but is also available to be shared with responders to

the extent they are capable of, and willing to, consume such content. This new multimedia content such as text, images, and video will require broadband wireless networks that have the appropriate capabilities to support these new media types. Thus, public safety broadband networks and NG911 systems will go hand-in-hand in serving public safety's future emergency response needs

One of the most critical issues that has yet to be resolved with respect to NG911 deployment is the identification of a secure source of funding that will promote quick and robust NG911 deployment and that will be sufficient to support the entire ecosystem of hardware, software, infrastructure, and processes that will need to be updated. Local, state, and regional public safety entities should consider whether there would be benefits to coordinating their NG911 and public safety broadband network deployments to avoid any duplication of efforts, to ensure compatibility, and to best leverage shared resources. However, the public safety broadband network will be essential to all aspects of public safety communications, of which 9-1-1 is only one component, and no delays to public safety broadband deployment should be permitted to arise because of conflation with NG911.

Broadband and NG911 applications should be provided at the optimal level to accommodate public safety operational needs. Control of content and applications very often needs to be at the local level. For example, NG911 systems will enable the collection and sharing of medical and other personal information that will improve the efficiency of emergency services but also raise concerns about privacy and confidentiality. Ultimately, local emergency response agencies need to maintain control over how personal information is collected and disseminated.

Specifically, the Commission seeks comment on how best to ensure that the public safety broadband network can adequately interconnect with NG911 networks. There should be appropriate convergence and sharing of equipment on a network level. Jurisdictions contemplating procurements of ESInets should make sure that their technical planning is done in the spirit with which the ESInet concept was developed in the first place, that of a shared network resource that accommodates not only 9-1-1 traffic, but that of first responder and other emergency services as well. Network capacity planning, network operations, security engineering, and resource sharing between and among agencies all need to be considered when a jurisdiction starts planning to procure and operate an ESInet. Appropriately engineered networks that provide differentiated QoS will allow Emergency Services IP Networks (ESInets) to accommodate other mission critical services, such as public safety broadband. One of the challenges of building an ESInet is the sizing required to handle a Denial of Service attack and still be able to process calls. The converged networks should be able to support Radio over IP traffic as well.

The Commission also inquires as to compatibility between the NG911 standards being developed and the contemplated technical architecture of the public safety broadband network. Motorola Solutions is not aware of any conflicts between the two. NENA has an effort underway called ESInet Network Design (ESIND) which addresses NG911 network design considerations. The CSRIC 4B NG911 Transition report refers to ESIND for network NG911 design considerations as well. This work by NENA has been explicitly carried out with the idea in mind of an ESInet as shared resource that carries more than 9-1-1 traffic, so the concept of

shared resources among 9-1-1 and first responders is built in to the ESInet concept. Adopting common underlying network technologies such as MPLS will ensure compatibility and sharing of networks where appropriate.